District Operations Guide

KETS Exchange 2003 / Windows Server 2008 Active Directory Environment

May 13, 2008
Last Updated: January 4, 2010
Version 3.6

Department of Education
Office of Education Technology,
Division of KETS Operations and Services
15 Fountain Place
Frankfort, KY 40601
502/564-2020

Revision History

This revision history is updated each time this document is updated. The history identifies the version number, the date the version was completed, the author of the changes, and a brief description of the changes.

Version	Date	Updated By	Description of Change
1.0.1	11/18/05	Debbie Lowery	Pg 23, item E-add the words email address to:"The provisioning system will create the distribution group **email address** during its next execution."
1.0.1	11/18/05	Debbie Lowery	Section 3.3.2-Add sentence to end of Note section. "For more information refer to section 3.2.3, section D.
2.0	03/08/06	Lisa Brewer	▪ Moved Revision History to separate page ▪ Updated Table of Contents ▪ Updated the following sections: ○ 1.2 ○ 3.1 ○ 3.2.1.1 ○ 3.2.2 ○ 3.2.3 ○ 3.2.4 ○ 3.2.6 ○ 3.3.1.d ○ 3.3.2 ○ 3.3.3 ○ 3.3.4 ○ Added 3.3.6 ○ 3.4.2 ○ 3.4.5 ○ 3.4.7 ○ 3.4.9.g ○ 3.4.10 ○ 4.1.1 ○ 4.1.2 ○ 5.1.2 ○ 5.1.3 ○ 5.2.1 ○ 6.1.2.2 ○ 6.1.3.1 ○ 7.3.1 ○ 8.1.5
3.0	05/13/08	MADS Team	3.2.3 – Added Dist Exchange Maintenance Reviewers Group 3.3.1 – Updated Formatting 3.4.10 - Added section to reference the section on Exchange System Manager

Version	Date	Updated By	Description of Change
3.0	05/13/08	MADS Team	5.1.1 – Revised method of obtaining Exchange System Manager. 5.1.1.1 – section added to describe Exchange System Manager usage. 5.1.2 – Added Exmerge check mailbox size procedures.
3.0	05/13/08	MADS Team	6.1.2.3 – Revised Client Browser for OWA support. 6.1.3.1 – Highlight note to disable cert. check.
3.0	05/13/08	MADS Team	7. - Added Increase mailbox size limit best practice and personal folder usage. 7.2.1 - Message Size Limitation to remain in place. 7.4.2 – changed EDdistrictnumberFEX 1 to ED###OWAFEX1. 7.6 – Changed point of contact to request SMTP Relay requests.
3.0	05/13/08	MADS Team	8.1.1 – removed reference to personal users
3.0	05/13/08	MADS Team	9.1.1 – Modification of Background statement. 9.1.1.1- Changed Item A to reflect Exchange Hosted Services.
3.0	05/13/08	MADS Team	Added Appendix A – B
3.0	6/12/09	MADS Team	4.1.1.2 – Added info about Exchange backups for districts who have been migrated to Windows Server 2008.
3.2	10/27/09	John Logan	Added Section 3, which discussed Windows Server 2008 specific functionality. This is a temporary addition until we get to the next generation of e-mail.

3.3	10/27/09	John Logan	Additional edits on Terry Orr's review
3.4	11/13/09	John Logan	After additional review by Terry. Removed DR AD
3.5	12/07/09	John Logan	Added Chris Hornfeldt section about replacing workstations (4.3.6)
3.6	1/04/10	John Logan	Modified Section 6.1 to reference 6.4.1 for System Manager install instead of contacting the Service Desk.

Table of Contents

1 Introduction

Welcome to the KETS Exchange Server 2003 / Windows Server 2008 Active Directory District Operations Guide. This guide is intended for the technical administrators of Kentucky school districts' Exchange 2003 systems as well as user administrators of Active Directory (AD) services. This guide describes the AD and Exchange environment and provides instructions for carrying out the routine operations required to administer these systems.

1.1 If You Need Help

In general, e-mail client operations in the KETS Exchange 2003 environment work as described in vendor documentation and Help screens. However, many server operations have been customized for the KETS environment and must be carried out as described in this document or in consultation with OET. If you are not sure whether vendor documentation is correct for a particular task, please contact the KETS Help Desk.

If you need assistance with the tasks described in this document, please contact the KETS Help Desk unless the task description instructs you otherwise.

1.2 Document Feedback

If you have ideas for improving this document, such as adding additional information or clarifying existing content, please send them to your KETS Engineer so they can be considered for future versions.

1.3 Document Updates

This document will be updated and enhanced over time. Please check for new versions periodically at
http://www.education.ky.gov/KDE/Administrative+Resources/Technology/KETS+Help+Desk/How+Tos+and+Standards+Documents/

You can check the version number that appears in the footer to determine if the posted version is newer than what you already have.

2 OET and District Responsibilities

OET is responsible for most technical maintenance and support of systems in the KETS Active Directory and Exchange environment, but districts are responsible for many administrative and end-user support tasks.

2.1 OET Responsibilities

OET is responsible for:

- Disaster recovery
    - Backups (one day on the server for Exchange)
    - Rebuilds/Restores
- Exchange and related software monitoring, upgrades, and patches
- Exchange server hardware monitoring, upgrades, and patches
- Exchange server operating system monitoring, antivirus protection, upgrades, and patches
- Exchange server-related problem diagnosis and resolution
- Exchange e-mail virus protection
- Enterprise support
    - Configuration Management
    - Address Lists
    - Enterprise-wide Standards and Policies
    - User Provisioning

2.2 District Responsibilities

Districts are responsible for:

- Exchange server power and network connectivity
- Exchange server machine environment (secure, clean, temperature-controlled location)
- User administration
- Archival backups and (if desired) off-server/offsite disaster-recovery backups
- User data backups and recovery

3 Windows Server 2008 Active Directory Specific Functionality

The KETS Active Directory (AD) environment is built on Windows Server 2008 Domain Services. Users rely on DNS within AD as well as 'external' DNS when required. Active Directory is responsible for user authentication and authorization throughout many services within the district environment. AD is also responsible for DHCP as well as other services.

The design of Active Directory for KETS exists as a classic hub-and-spoke topology, consisting of an 'empty' root domain (KETSDS.NET) with 179 sub-domains. AD replication is linear from each district domain to the hub-site, replicating on a one-hour interval. Each district domain has two AD Domain Controllers which reside physically within the district on OET managed hardware. Each district also has an additional AD Domain Controller which resides at OET.

With the recent migration to Windows Server 2008 Domain Services (Active Directory) there are a couple of specific new technologies that districts should make themselves aware of. These are outlined below.

3.1 Directory Service Performance and Availability

In every district there are physically two servers which provide Active Directory Domain Controller roles, one being a Global Catalog which is used primarily for Universal Security Group membership lookups at logon. Additional Global Catalog servers exist throughout the state in the event that the 'local' GC is down the end user can traverse the network to access GC resources. These two 'servers' exist in a virtual environment, with more than twice the resources of the Windows 2003 domain controllers (RAM, CPU, etc). RAID level 10 is utilized for the database which provides optimal IOPS.

3.2 Password Policies

In Windows Server 2003 Active Directory a domain was a password policy boundary meaning that a single password policy applies to all users in an Active Directory domain. There is a new technology in Windows Server 2008 Domain Service (Active Directory) called **Fine-Grained Password Policies** which enables the use of granular password policies for subsets of users within a domain. This new technology is an extension of the existing Default Domain Password Policy (explained later). Districts have the ability to utilize any of six new policies for different groups of users.

A district can choose to utilize only the default domain policy but will have the ability to take certain groups of users, students for example, and apply different password policies from the staff. The Default Domain Password Policy affects all users in a domain that are not members of one of the Fine-Grained Password Policy Groups. These new policies are not implemented on an OU basis. They are assigned to security groups and/or users (discussed below).

Fine-Grained Password Policies work with the Default Domain Password Policy through 'precedence' or weighting. The Default Domain Password Policy has the lowest weight, meaning if a user is placed in any of the password policy groups (explained below) the group policy will be applied instead of the Default Domain Password Policy. The groups have weighting as well, so users can be in multiple groups but only the group policy with the highest weighting will be applied to that user.

If a district chooses to utilize the Default Domain Password Policy they must ensure that it meets the minimum requirements for mailbox access. If a district would like to utilize the default policy and needs to modify it they need to contact the KETS Service Desk.

Six new Global Security Groups created which will reside in the *_District Admins, Users and Groups OU.* For a given policy to be applied users must be placed in that corresponding group. The groups and explanation of each follow.

DIST Password Policy - None

This policy requires no minimum password length, no complexity, forces no change and has a zero password history.

DIST Password Policy - Three Never

This policy requires a three character password length minimum, no complexity, forces no change and has three passwords remembered (meaning you cannot reuse the last three passwords)

DIST Password Policy - Six Never

This policy requires a six character password length minimum, no complexity, forces no change and has a zero password history

DIST Password Policy - Six Complex 60

This policy requires a six character password length minimum, forces complexity*****, forces a change at 60 days and has five passwords remembered (meaning you cannot reuse the last five passwords)

DIST Password Policy - Eight 60

This policy requires an eight character password length minimum, no complexity, forces a change at 60 days and has three passwords remembered (meaning you cannot reuse the last three passwords)

DIST Password Policy - Eight Complex 30

This policy requires an eight character password length minimum, forces complexity*, forces a change at 30 days and has twelve passwords remembered (meaning you cannot reuse the last twelve passwords)

* For those policies above which require complexity the user must meet at least three of the following four complexity rules within the password:

- Uppercase characters (A through Z)
- Lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Special symbols or non-alphabetic characters (for example: !, $, #, %, etc.)

The precedence of these groups goes from the lowest precedence "**DIST Password Policy – None"** to the highest precedence "**DIST Password Policy - Eight Complex 30"**. This is with the understanding that the Default Domain Password Policy ultimately has the lowest precedence. To that end if a user is a member of any of these groups the group policy is applied instead of the Default Domain Password Policy. Also, if there are settings defined on the actual user object ('Password Never Expired', etc) those settings will apply no matter what policy the user is associated with.

Example: If a user is in both the '**DIST Password Policy - Three Never'** group and the '**DIST Password Policy - Eight 60'** group the user would have to meet the requirements of the DIST Password Policy – Eight 60 group.

When a user is placed in a Fine-Grained Password Policy group, or if the Default Domain Password Policy is modified, the affected users will NOT be required to immediately

change their password to match the minimum requirements. The next time the user will have to change their password the new policy would be applied at that time. If a user currently has no password policy that requires them to change their password the user would either have to be instructed to change their password manually or the user object would need to be set to 'User must change password at next logon'. This can be accomplished either in Active Directory Users and Computers on a per user basis or through a script (VB, LDIFDE, etc) which would modify the pwdLastSet attribute to 0 (zero) on each user object. District will also have the ability to change the password on behalf of the user through whatever means they may do this today.

NOTE: There appears to be a 'bug' with Fine-Grained Password Policies in that the message that some clients will receive when changing their password can be different than what should be presented. Some versions of Windows tested (Windows 7, Vista) provided a generic message when a user password change was attempted that didn't meet the minimum requirements of the Fine-Grained Password Policy:

Unable to update the password. The value provided for the new password does not
meet the length, complexity, or history requirement of the domain.

This isn't very helpful, but it's acceptible in that it doesn't provide inaccurate information. Also it is good for security reasons as it doesn't show a person trying to guess another users password any minimum requirements. It's important to note that all versions/service packs were not tested, only Windows 7 RC and Vista Ultimate SP2. Other versions may react differently, possibly as described below. It's also important to note that the Fine-Grained Password Policies all worked well functionally in testing, the only issue as explained here it the message that results from a user trying to change their password to something that doesn't meet the resultant policy for that user.

With Windows XP SP3 testing results were different. Testing results:

If a user has a Fine-Grained Password Policy assigned and tries to change their password to a password that doesn't meet the minimum requirements of the FGPP that user will receive a popup (which is expected), but the information in the popup applies to the Default Domain Policy settings, not the Fine-Grained Password Policy settings that the user actually is held to.

Example: The Default Domain Password Policy for your district is 6 character, 0 history and 0 min days. You assign a user to the 'DIST Password Policy – Three Never' group. This policy is the same as the default domain policy, other than the password length must be at least 3 characters instead of 6 in length. If the users tries to change their password to a password that is 2 characters in length they will receive the following message:

This is incorrect, as the user in the example would only need to supply a password of 3 characters as a minimum. This is the same if the user was placed in the 'DIST Password Policy – Eight Complex 30' group, which requires a password of at least 8 characters, complexity enabled and a 30 day maximum age. If a person in this group tried to change their password to something that didn't meet the requirements, say only 7 characters, it would still present the above image which again is incorrect and will cause confusion.

OET has worked with Microsoft to have this documented in its own whitepaper as a very brief and poor description of this issue is currently 'buried' in an obscure location in another document. It must be advised that if districts wish to utilize Fine-Grained Password Policies this will be an issue for some users/clients, as currently an estimated 90% of clients in KETS would receive this 'incorrect' message.

3.3 Group Policy Preferences

Windows Server 2008 Domain Services has a new feature called Group Policy Preferences. Group Policy Preferences , which are not 'required' policies, but settings which end users can choose to apply or not. The main difference between Group Policies and Group Policy Preferences is how they are enforced (or not enforced).

The table below was pulled from the 'Group Policy Overview' document. Group Policy Preferences allow for users of the policies to have flexibility on whether they want the policy applied or not.

	Group Policy Preferences	Group Policy Settings
Enforcement	• Preferences are not enforced • User interface is not disabled • Can be refreshed or applied once	• Settings are enforced • User interface is disabled • Settings are refreshed
Flexibility	• Easily create preference items for registry settings, files, and so on • Import individual registry settings or entire registry branches from a local or a remote computer	• Adding policy settings requires application support and creating administrative templates • Cannot create policy settings to manage files, folders, and so on
Local Policy	• Not available in local Group Policy	• Available in local Group Policy
Awareness	• Supports non-Group Policy-aware applications	• Requires Group Policy-aware applications
Storage	• Original settings are overwritten • Removing the preference item does not restore the original setting	• Original settings are not changed • Stored in registry Policy branches • Removing the policy setting restores the original settings
Targeting and Filtering	• Targeting is granular, with a user interface for each type of targeting item • Supports targeting at the individual preference item level	• Filtering is based on Windows Management Instrumentation (WMI) and requires writing WMI queries • Supports filtering at a GPO level
User Interface	• Provides a familiar, easy-to-use interface for configuring most settings	• Provides an alternative user interface for most policy settings

For more information on Group Policy Preferences please refer to:

http://www.microsoft.com/DownLoads/details.aspx?familyid=42E30E3F-6F01-4610-9D6E-F6E0FB7A0790&displaylang=en

http://technet.microsoft.com/en-us/library/cc731892(WS.10).aspx

4 Users and Mailboxes

In the KETS Exchange 2003 environment, users and mailbox configuration data are stored within Active Directory; therefore, user and mailbox management are carried out using Active Directory tools. While some procedures can be completed with the basic Active Directory Users & Computers program (ADUC), many can only be completed using a computer on which ADUC has been enhanced by installing the Exchange 2003 System Management Tools. Instructions for installing these tools can be found in section 5.2.1, "Install Exchange 2003 System Management Tools."

4.1 Provisioning

When a new user is created in Active Directory, or certain changes are made to an existing user in Active Directory, the provisioning system is responsible for creating or modifying the corresponding Exchange 2003 mailbox. An OET-maintained provisioning script executes every weekday (5 days a week) at 7 pm local time on each district's Exchange 2003 system to check for changes to Active Directory and make the appropriate corresponding changes in the Exchange 2003 system.

Note: *All Active Directory changes must be made between 7 AM and 6 PM local time in order for the scheduled script to make the related Exchange 2003 changes by the following morning.*

4.2 Active Directory and Exchange 2003 Background

4.2.1 Types of Objects

The following types of objects are used in the KETS Exchange 2003 environment. Note that while some of these objects are Microsoft-defined Active Directory object types, others are defined only within the KETS Exchange 2003 environment.

Exchange mailboxes are not AD objects.

4.2.1.1 User

In the KETS Exchange 2003 environment, user objects are used in two ways:

a. Personal User – to represent an individual human user who will log in to the AD and Exchange systems.

b. Resource User – to represent a service, schedulable resource, or shared mailbox; for instance, a database server, a conference room or a shared webmaster mailbox to which multiple human users need access.

Within this document the term "user" refers to the AD user object, including both personal and resource users; in those cases in which personal and resource users are handled differently the document will specify the type.

4.2.1.2 Contact

An Active Directory contact object has some descriptive attributes, including an e-mail address, but does not have a mailbox, cannot be assigned permissions, and does not have login credentials. In the KETS Exchange 2003 environment, contact objects are used to provide GAL and address list entries for persons/resources that have mailboxes outside the KETS Exchange 2003 environment; for instance, for staff of state agencies other than KDE. Contacts are similar to Exchange 5.5 custom recipients.

4.2.1.3 Group

There are several varieties of Active Directory group objects.

a. Distribution group – an object representing a group of mail-enabled objects but which cannot be assigned permissions; a message sent to the distribution group is automatically sent to all the members. The provisioning system will make all distribution groups into Universal groups regardless of the choice made when the group is created. Distribution groups are similar to Exchange 5.5 distribution lists.

b. Security group (not mail-enabled) – an object representing a group of objects; permissions granted to the group are automatically available to all the members of the group. Security groups which are not intended to be used as e-mail destinations must NOT be placed in any of the mail-enabled OUs (described below); they can be placed in the **_Groups** OU described below or in other OUs outside the mail-related OU hierarchy.

c. Security group (mail-enabled) – an object representing a group of mail-enabled objects which can both be assigned permissions and used as an e-mail destination. A security group is made mail-enabled by placing it in one of the mail-related OUs described below. The provisioning system will make all mail-enabled security groups into Universal groups regardless of the choice made when the group is created; if a security group's scope needs to be Domain Local or Global, you should not place it in any of the mail-related OUs and therefore it will *not* be mail-enabled.

4.2.1.4 Query-based Distribution Group

A query-based distribution group is an object representing a group of mail-enabled objects; a message sent to the distribution group is automatically sent to all the members. Unlike an ordinary distribution group or a mail-enabled security group, you do not manually adjust the membership of a query-based distribution group; instead, you define a query which chooses certain objects from Active Directory. The query is executed each time a message is sent to the query-based distribution group. Query-based distribution groups must be used with caution because they use significant Exchange and Active Directory resources.

4.2.2 Distribution Groups

Distribution groups are used to simplify sending e-mail to groups of mail-enabled objects.

***Note**: All Distribution Groups migrated from Exchange 5.5 Distribution Lists must be reviewed after migration. The Owner and Delivery Restrictions do not migrate along with the group. You must manually add these back to each distribution group.*

4.2.2.1 KETS Exchange 2003 Notification Distribution Groups

The following distribution group is used to support the administration of your Exchange 2003 system. It is located within the **Users and Groups** sub-OU of the **_District Admins** OU and should not be modified, though you may change its membership.

- **DIST Email Antivirus Notification** – any AD user, distribution group, mail-enabled security group, or contact object which is added to this group will receive an e-mail alert when the GroupShield software on your Exchange 2003 system discovers a virus.

4.2.2.2 KDE-Required Distribution Groups

KDE requires districts to maintain certain distribution groups to support sending messages to teachers, principals, etc. statewide. OET creates and modifies KDE-required distribution groups but you are expected to keep the membership up to date. These distribution groups are located within the **_Exchange Resources** sub-OU of the **Leadership** OU. The groups are:

- All *District* Supt
- All *District* Prin
- All *District* EL Prin
- All *District* MS Prin
- All *District* HS Prin
- All *District* Teachers
- All *District* EL Teachers
- All *District* MS Teachers
- All *District* HS Teachers
- All *District* IT Teachers
- All *District* KVHS (and subsequent KVHS DGs per school where applicable)

where *District* refers to District Name, with either Co for County or Ind for Independent (with no ending period).

Examples:

- All Franklin Co Supt
- All Frankfort Ind EL Prin

4.2.2.3 District Distribution Groups

You may create distribution groups for internal district use; see the descriptions of OUs found below to determine the proper OU.

4.2.3 Security Groups

Security group membership is used to control user access and activity for both e-mail end users and administrators. The Exchange-related security groups, which are not mail-enabled, are located within the **Users and Groups** sub-OU of the **_District Admins** OU and should not be modified, though you may change their membership. The security groups are:

DIST Support Admins – any AD user object which is in this security group can perform all the mail-related operations described in this document *except* directly modify e-mail addresses and add/modify contact objects; for those tasks the user must be a member of one of the All Mailbox Access security groups described below.

a. **DIST Staff User Admins** – any AD user object which is in this security group can perform all the mail-related operations described in this document within the **Staff** and **Leadership** OUs and their sub-OUs *except* directly modify e-mail addresses and add/modify contact objects; for those tasks the user must be a member of one of the All Mailbox Access security groups described below.

b. **DIST Student User Admins** – any AD user object which is in this security group can perform all the mail-related operations described in this document within the **Students** OU and its sub-OUs *except* directly modify e-mail addresses and add/modify contact objects; for those tasks the user must be a member of one of the All Mailbox Access security groups described below.

c. **DIST Staff District Email Only** – any AD user object that is in the **Staff** or **Leadership** OU (or any of their sub-OUs) and which is added to this security group will only be able to send and receive e-mail within the district. The change will take effect immediately.

d. **DIST Students District Email Only** – any AD user object that is in the **Students** OU (or any of its sub-OUs) and which is added to this security group will only be able to send and receive e-mail within the district. The change will take effect immediately.

e. **DIST Staff All Mailbox Access** – any AD user object which is added to this security group will be able to open any and all mailboxes that are related to AD user objects that are located in the **Staff** or **Leadership** OUs (or any of their sub-OUs); this can be used to inspect a particular mailbox or to export mailbox content. Members of this security group can also add contact objects and update e-mail addresses within the **Staff** and **Leadership** OUs (any any of their sub-OUs). The access provided by this group will take effect the next time the user logs in to the domain.

f. **DIST Students All Mailbox Access** – any AD user object which is added to this security group will be able to open any and all mailboxes that are related to AD user objects that are located in the **Students** OU (or any of its sub-OUs); this can be used to inspect a particular mailbox or to export mailbox content. Members of this security group can also add contact objects and update e-mail addresses within the **Students** OU (and any of its sub-OUs). The access provided by this group will take effect the next time the user logs in to the domain.

g. **DIST Exchange Maintenance Reviewers -** any AD user object which is added to this security group will have read-only access to maintenance-level information on the district exchange server. Exchange System Manager can be used to perform message tracking, view local SMTP Queues, along with viewing mailbox sizes and disconnected mailboxes. The access provided by this group will take effect the next time the user logs in to the domain.

h. **DIST Public Folder Admins** – (optional) any AD user object which is added to this security group will have the ability to manage your district's public folders. In addition, this group will own all of your district's public folders. This security group will only be created for districts that are using public folders. The access provided by this group will take effect the next time the user logs in to the domain. ***Note:*** *This group should not be used to give end users access to individual folders; that type of access is granted using the permissions tab of the public folder (using the Outlook client).*

***Note: For the following groups to function as designed, each should contain only user objects. Nested groups are not allowed. If you add users to a group and add that group to any of these groups they will not function correctly*.**

i. **DIST Staff Deleted Mailboxes** – any AD user object that is in the **Staff** or **Leadership** OU (or any of their sub-OUs) and which is added to this security group will not have a related mailbox created for it. If the AD user object currently has a related mailbox, the mailbox will be deleted by the provisioning system. The AD user object may still be used for other tasks, such as accessing file servers. To reverse this configuration and have the mailbox recreated, remove the user from the security group.

j. **DIST Staff Locked Mailboxes** – any AD user object that is in the **Staff** or **Leadership** OU (or any of their sub-OUs) and which is added to this security group will not be able to access its related mailbox after the provisioning system's next execution. The mailbox will not be removed from the system. Although the mailbox is inaccessible to the user, all mail destined for the mailbox will be delivered. The AD user object may still be used for other tasks, such as accessing file servers. **Important Note**: To reverse this configuration and give the user access to their mailbox, remove the user from the security group.

k. **DIST Students Deleted Mailboxes** – any AD user object that is in the **Students** OU (or any of its sub-OUs) and which is added to this security group will not have a related mailbox created for it. If the AD user object currently has a related mailbox, the mailbox will be deleted by the provisioning system. The AD user object may still be used for other tasks, such as accessing file servers. To reverse this configuration and have the mailbox recreated, remove the user from the security group.

l. **DIST Students Locked Mailboxes** – any AD user object that is in the **Students** OU (or any of its sub-OUs) and which is added to this security group will not be able to access its related mailbox after the provisioning system's next execution. The mailbox will not be removed from the system. Although the mailbox is inaccessible to the user, all mail destined for the mailbox will be delivered. The AD user object may still be used for other tasks, such as accessing file servers. *Important Note:* To reverse this configuration and give the user access to their mailbox, remove the user from the security group.

Note*: Two special Exchange-related security groups,* ***'Exchange Domain Servers'*** *and* ***'Exchange Enterprise Servers',*** *which are located within the* ***Users*** *OU should not be modified and must be preserved.*

Note*: The* ***'Exchange Domain Servers'*** *and* ***'Exchange Enterprise Servers'*** *security groups must not be deleted or moved; such changes will render the district Exchange 2003 server inoperable. If the groups are deleted, then the district will have*

to work with KDE to restore the groups. Until restored, all messaging functions at the district will be unavailable.

Moving the aforementioned groups has the same effect. Although moving them back is a trivial procedure, Exchange 2003 will be inoperable until such move takes place.

4.2.4 Required Object Attributes

The required attributes of Active Directory user objects must have correct values. Use mixed case (John Doe, not JOHN DOE or john doe) for the first and last names of personal users.

a. Students

The following fields must be filled in correctly for students:

- First Name
- Last Name
- Department – must contain expected four-digit high school graduation year (like 2014).

  All other fields that display in the Address Book must be blank in order to meet FERPA and Kentucky requirements for privacy of student information.

b. Staff

The following fields must be filled in correctly for staff (including Leadership):

- First Name
- Last Name

c. Resource

No specific fields are required for resource objects. Note that if the first name and last name fields are not filled in for a resource object, the SMTP prefix will be the same as the object's logon name.

***Note**: The special character "/" (forward slash) cannot be used in the following attributes: Name, First Name, Last Name and Alias. Additionally, the "/" cannot be used in the Leadership, Staff and Student sub-OU names*

4.2.5 Optional Extension Attributes

Districts will be able to use five Active Directory extension attributes on mail-enabled objects of any kind (user, distribution group, mail-enabled security group, contact). These fields do not appear in any global address list or other address list and are useful for information that should not be publicized. The use and format of these fields will not be standardized by KDE and is completely at your discretion. The attributes are:

- ExtensionAttribute1
- ExtensionAttribute2
- ExtensionAttribute3
- ExtensionAttribute4
- ExtensionAttribute5

These attributes can only be edited from a machine on which the Exchange 2003 System Management Tools are installed.

Extension attributes six through fifteen are reserved for KDE use. These attributes may eventually have standard meanings and formats.

4.2.6 Organizational Units

The following organizational units (OUs) are used to contain Active Directory objects that need e-mail functionality. OU membership affects address list visibility and mailbox size limits. Note that the address list visibility described below only applies to end users using standard MAPI clients and Outlook Web Access; for information about other clients see Section 8, "Address Lists."

***Note**: The special character "/" (forward slash) cannot be used in the Leadership, Staff and Student sub-OU names*

a. **Leadership** – this OU is intended for leadership personal user objects, which should be used for staff members who need higher mailbox size limits. The total number of user objects allowed in this OU is either 10 or 2 times the district workstation allocation (DWA), whichever is higher. The mailboxes associated with AD user objects in this OU will have the leadership/staff e-mail address format, a size limit of 200 MB, and will appear to staff throughout the state and students within the district, but not to students outside the district (formerly Trust Level 15).

b. _**Exchange Resources** within **Leadership** – this OU is intended for

- Leadership-related resource user objects (such as a webmaster mailbox). Resource user objects in this OU will have the leadership/staff e-mail address format, a size limit of 200 MB, and will appear to staff and students within the district, but not to anyone outside the district (formerly Trust Level 20).
- Leadership-related distribution group, mail-enabled security group, and query-based distribution group objects. Such objects in this OU will have the leadership/staff e-mail address format and will appear to staff and students within the district, but not to anyone outside the district (formerly Trust Level 20).
- Leadership-related contact objects. AD contact objects in this OU will appear to staff and students within the district, but not to anyone outside the district (formerly Trust Level 20).
- KDE-required distribution group objects. KDE-required distribution group objects placed and maintained in this OU by OET will appear to staff throughout the state and students within the district, but not to students outside the district (formerly Trust Level 15). You should not modify KDE-required distribution group objects other than to add or remove members appropriately. See section 3.2.2.2, "KDE-Required Distribution Groups" for more information.

c. **_Groups** within **Leadership** - objects in this OU will not be provisioned for e-mail in any way. This OU can be used for security groups that should not be mail-enabled.

d. Other OUs within **Leadership** – any other OU that is a sub-OU of **Leadership** (but not a sub-OU of **_Exchange Resources** or **_Groups**) has the same behavior as the **Leadership** OU.

e. **Staff** – this OU is intended for staff (non-leadership) personal user objects. The mailboxes associated with AD user objects in this OU will have the leadership/staff e-mail address format, a size limit of 45 MB, and will appear to staff throughout the state and students within the district, but not to students outside the district (formerly Trust Level 15).

f. **_Exchange Resources** within **Staff** – this OU is intended for

- Staff-related resource user objects (such as a conference room). Resource user objects in this OU will have the leadership/staff e-mail address format, a size limit of 45 MB, and will appear to staff within the district, but not to students within the district or to anyone outside the district (formerly Trust Level 14).
- Staff-related distribution group, mail-enabled security group, and query-based distribution group objects. Such objects in this OU will have the leadership/staff e-mail address format and will appear to staff within the district, but not to students within the district or to anyone outside the district (formerly Trust Level 14).
- Staff-related contact objects. AD contact objects in this OU will appear to staff within the district, but not to students within the district or to anyone outside the district (formerly Trust Level 14).

g. **_Groups** within **Staff** - objects in this OU will not be provisioned for e-mail in any way. This OU can be used for security groups that should not be mail-enabled.

h. Other OUs within **Staff** – any other OU that is a sub-OU of **Staff** (but not a sub-OU of **_Exchange Resources** or **_Groups**) has the same behavior as the **Staff** OU.

i. **Students** – this OU is intended for student personal user objects. The mailboxes associated with AD user objects in this OU will have the student e-mail address format, a size limit of 5 MB, and will only appear to staff and students within the district (formerly Trust Level 20).

j. **_Exchange Resources** within **Students** – this OU is intended for

- Student-related resource user objects (such as an STLP Lab). The mailboxes associated with AD user objects in this OU will have the student e-mail address format, a size limit of 5 MB, and will only appear to students within the district (formerly Trust Level 19).
- Student-related distribution group, mail-enabled security group, and query-based distribution group objects. Such objects in this OU will have the student e-mail address format and will only appear to students within the district (formerly Trust Level 19).
- Student-related contact objects. AD contact objects in this OU will only appear to students within the district (formerly Trust Level 19).

k. **_Groups** within **Students** – objects in this OU will not be provisioned for e-mail in any way. This OU can be used for security groups that should not be mail-enabled.

l. Other OUs within **Students** – any other OU that is a sub-OU of **Students** (but not a sub-OU of **_Exchange Resources** or **_Groups**) has the same behavior as the **Students** OU.

4.3 Basic Procedures

In general, you can carry out the following procedures using any AD user that is a member of **DIST Support Admins, DIST Staff User Admins** (for actions within **Staff/Leadership** OUs), or **DIST Student User Admins** (for actions within **Student** OUs); exceptions will be noted.

4.3.1 Create a User with a Mailbox

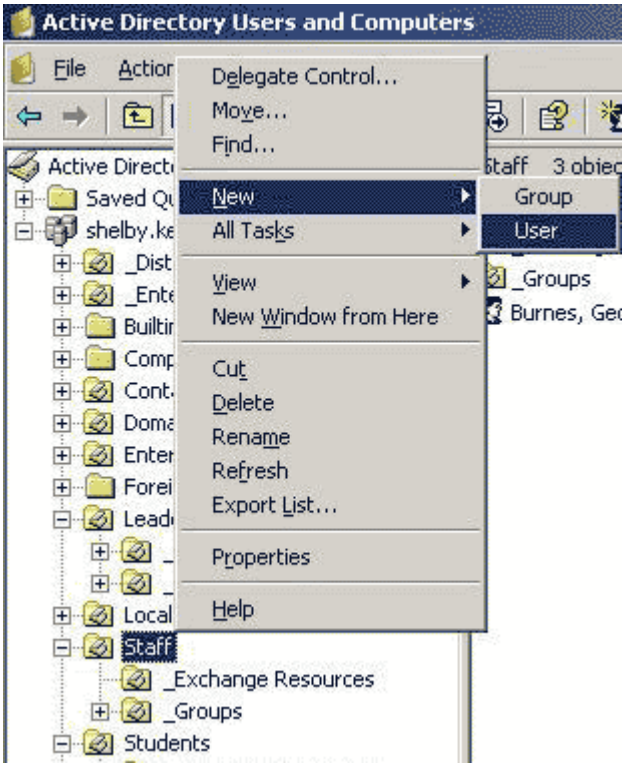
This procedure is used to create either a personal user or resource user; any differences are noted within the procedure.

Note: While this section does not describe the procedure, it is possible to create a new user by copying and modifying an existing user. However, in order to successfully do this you* must *use an XP machine on which the Exchange 2003 System Management Tools have been installed (see section 5.2.1, "Install Exchange 2003 System Management Tools").

a. Determine the OU for the new user based on the OU descriptions above. You may want to use a sub-OU of one of the defined OUs.

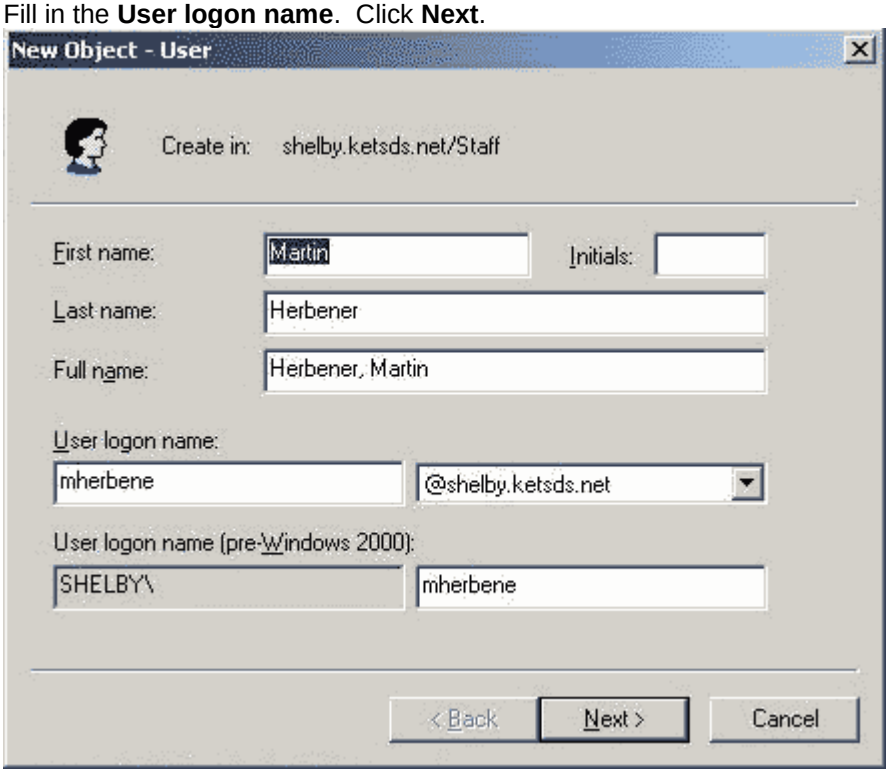
b. Open ADUC and navigate to the chosen OU.

c. Right-click on the chosen OU and choose **New > User.**



d. Choose between the following depending on whether you are setting up a personal user or resource user.

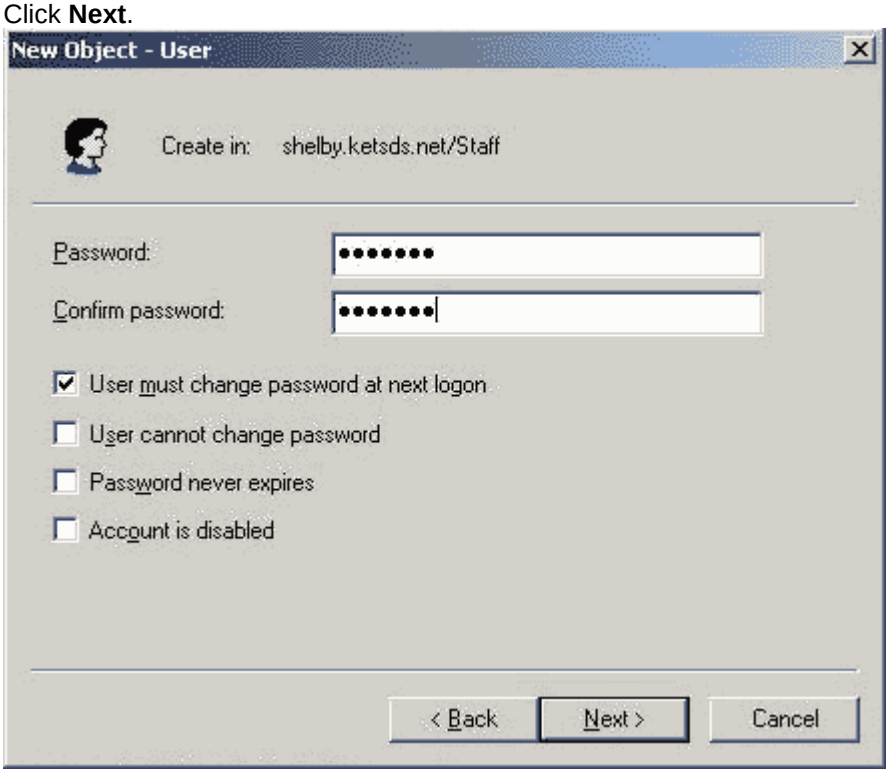
- Personal: Fill in the **First name** and **Last name** fields. The **Full name** field will be filled in automatically; this will be the display name that appears in the global address list and address lists. ***Note: While it is possible to manually edit the Full Name field, such changes are not recommended because the value entered here appears as both the Display Name* and *the user's name in ADUC. You may change these values after user creation is complete by following the instructions in section 3.4.3, "Change the Name of a Personal User".***
  Fill in the **User logon name**. Click **Next**.



- Resource: You may fill in the **First name** and **Last name** fields (in which case the **Full name** field will automatically be populated) or you may leave them blank and fill in only the **Full name** field. The **Full name** field will be the display name that appears in the global address list and address lists. If you do not fill in the **First name** and **Last name** fields, the **User logon name** will be used as the e-mail prefix (the part before the @ symbol in the SMTP address). Fill in the **User logon name.** Click **Next**.

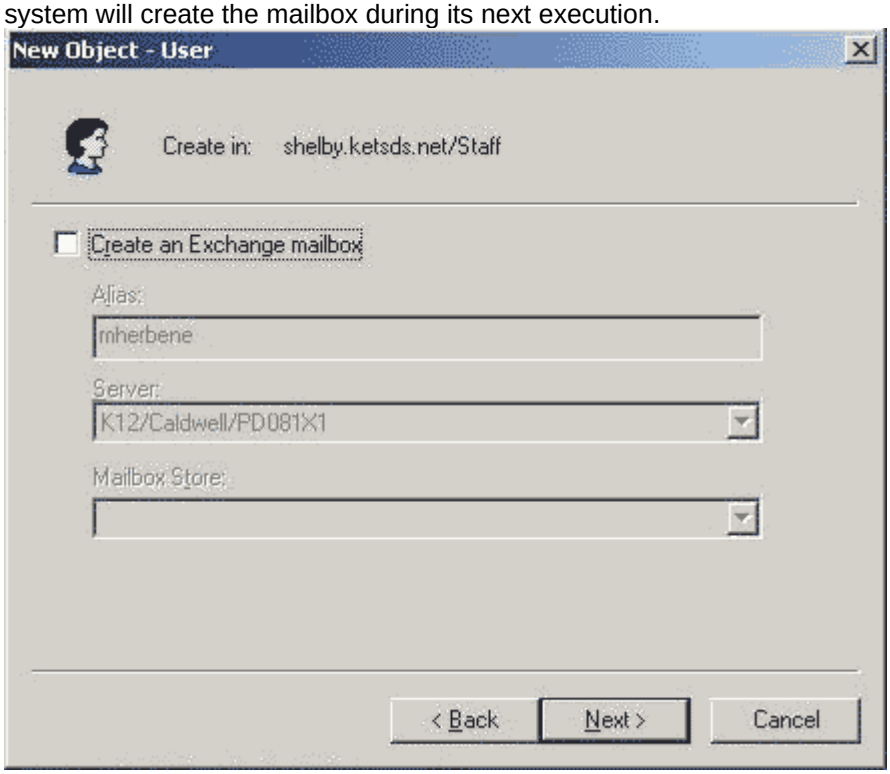
e. Choose between the following depending on whether you are setting up a personal user or resource user.

- Personal: Fill in the **Password** field with a temporary password and click the checkbox for **User must change password at next logon**. Click **Next**.



- Resource: Fill in the **Password** field with a strong (hard to figure out) password. Click **Next**

f. The next screen will appear with **Create an Exchange mailbox** checked. Click the checkbox for **Create an Exchange mailbox** to *uncheck* that option; it must be *unchecked* before you proceed and if you leave the option checked you will receive an error message. Click **Next** and finish the user creation process. The provisioning system will create the mailbox during its next execution.



4.3.2 Create a Mailbox for an Existing User

If a personal or resource user object does not currently have a mailbox because of its OU location, follow these steps to give it a mailbox. ***Note: if the object has been placed in the security group that prevents it from having a mailbox, this procedure will not change that fact; you will have to adjust the user's group membership. For more information refer to section 3.2.3, section D.*** Determine the OU to which you will move the object based on the OU descriptions in Section 3.2.6. You may want to use a sub-OU of one of the defined OUs.

a. Open ADUC and navigate to the OU that currently contains the object.

b. Move the user object to the determined OU by either dragging-and-dropping the object to the OU or by right-clicking on the object, choosing **Move**, and finding the new OU in the dialog box. The provisioning system will create the mailbox during its next execution.

4.3.3 Modify Object Visibility or Size Limit

If a user, distribution group, mail-enabled security group, or contact object does not have the correct visibility or (in the case of a personal user or resource user) mailbox size limit, follow these steps to carry out the appropriate modification. Note that moving an object from one OU to another can affect the application of AD Group Policies; make sure the destination OU's policies are appropriate for the object. Mailbox content will be preserved.

a. Determine the OU to which you will move the object based on the OU descriptions in Section 3.2.6. You may want to use a sub-OU of one of the defined OUs.

b. If you are moving a personal or resource user object to an OU with a lower mailbox size limit, ensure that the size of any existing mail content is under the limit of the destination OU.

***Note**: The mailbox will not move if its size is over the target OU mailbox size limit.*

c. Open ADUC and navigate to the OU that currently contains the object.

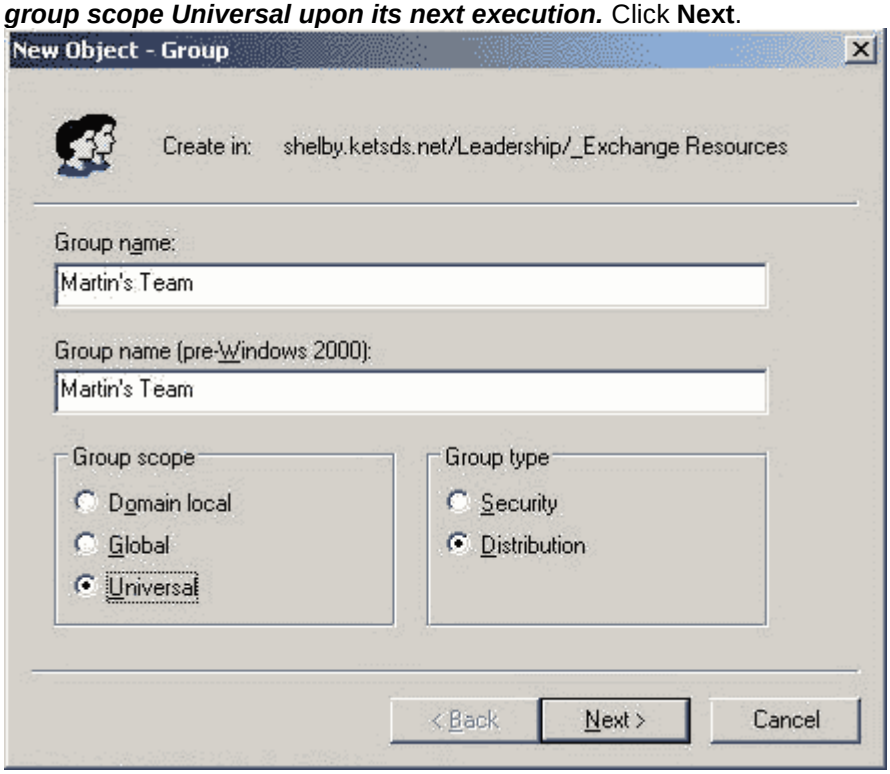
d. Move the object to the destination OU by either dragging-and-dropping the object to the OU or by right-clicking on the object, choosing **Move**, and finding the new OU in the dialog box. The provisioning system will modify mailbox size and visibility during its next execution.

4.3.4 Create a Distribution Group

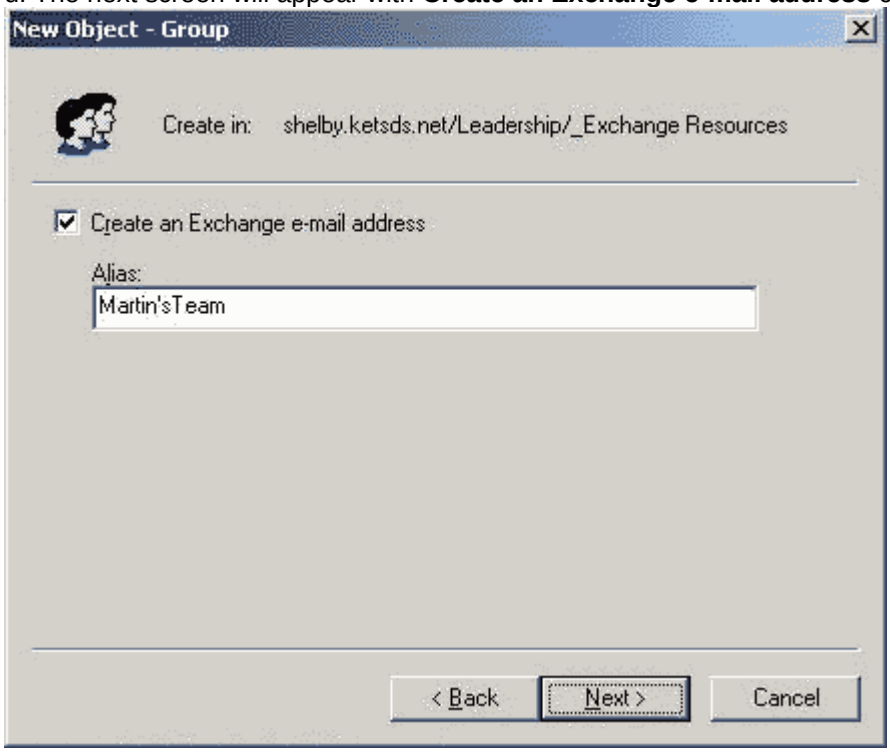
a. Determine the OU for the new distribution group based on the OU descriptions in Section 3.2.6. You may want to use a sub-OU of one of the defined OUs.

b. Open ADUC and navigate to the chosen OU. Right-click on the chosen OU and choose **New > Group**.

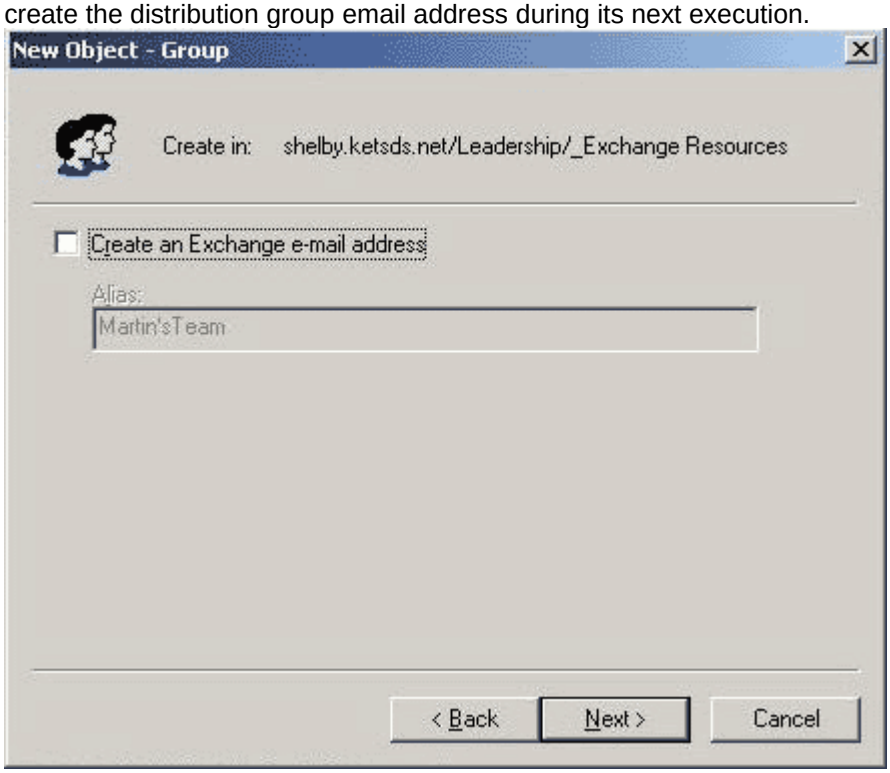
c. Fill in the **Group name** field; this value (with certain characters, such as spaces, removed) will become the prefix of the SMTP e-mail address. Choose **Universal** as the **Group Scope** and **Distribution** as the **Group Type**. ***Note: Even if you do not choose Universal as the type at this point, the provisioning system will make the group scope Universal upon its next execution.*** Click **Next**.



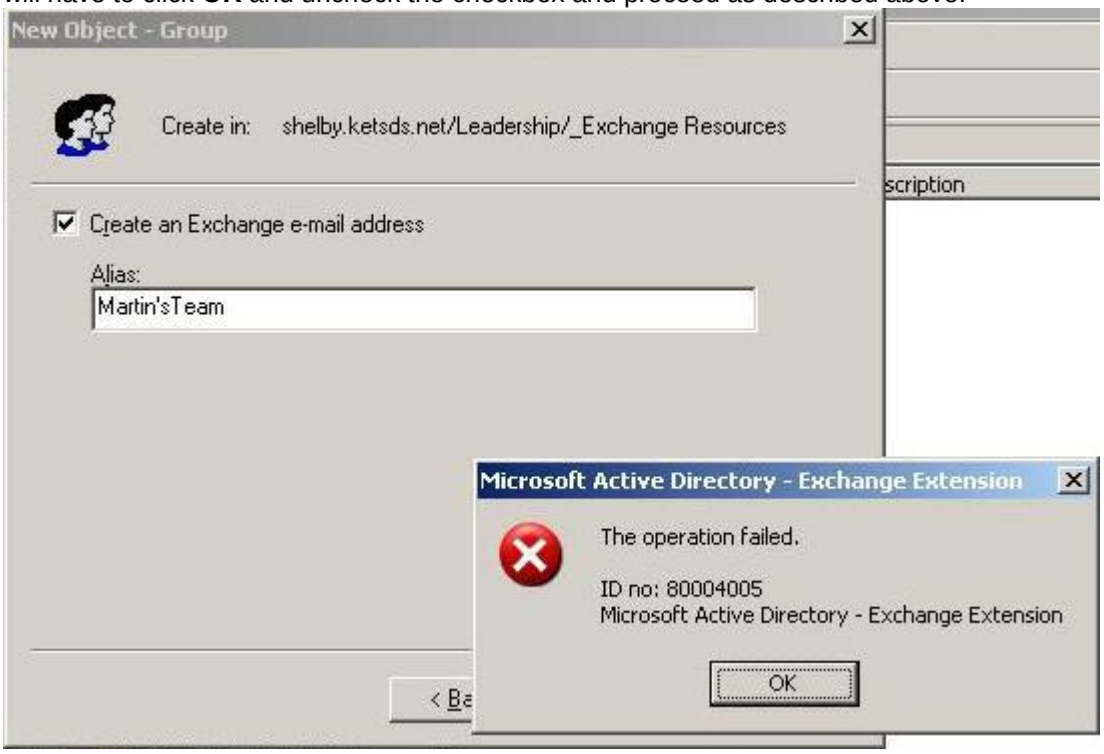
d. The next screen will appear with **Create an Exchange e-mail address** checked.



e. Click the checkbox for **Create an Exchange e-mail address** to *uncheck* that option; it must be *unchecked* before you proceed. Click **Next**. The provisioning system will create the distribution group email address during its next execution.



f. If you leave the checkbox checked you will receive the error message below; you will have to click **OK** and uncheck the checkbox and proceed as described above.



4.3.5 Delete a Group

This procedure is used to delete district distribution groups and security groups. Note that the distribution groups described in section 3.2.2.2, “KDE-Required Distribution Groups” will be created, modified and removed as necessary by OET; you should not attempt to modify them.

a. Open ADUC and navigate to the OU that currently contains the group.

b. Right-click on the group and choose **Delete**.

4.3.6 Replacing or Reimaging a Workstation/Server

Use this procedure when replacing or reimaging a system and using an existing computer object name. This process will allow the new/newly reimaged system to have update rights to existing AD Objects and DNS entries with the newly assigned SID (Security Identifier)

In order to carry out this procedure, you must have Active Directory Users and Computers installed.

a. Remove the existing computer from the network. Reimage or replace workstation.

b. Open ADUC and navigate to the OU containing the computer object. (ex. Office-PC)

c. Left click to highlight the computer account.

d. Right click the computer account and left click **RESET ACCOUNT**

e. Wait **15** minutes to allow the DC and GC to replicate the change.

f. Join the computer to the domain following the normal procedure. This system will be assigned a new SID and those permissions will be given to the existing DNS entry, Computer object, and DHCP lease.

NOTE: Deleting computer accounts instead of resetting will lead to stale/orphaned DNS entries which will not be cleared out until scavenging flushes the records 8 – 14 days after they go stale.

4.3.7 Public Folder Permissions

A top level public folder will be created for each district that chooses to use public folders. The owner of each top level district public folder should be the **DIST Public Folder Admins** security group.

By default, your top level district public folder should have the following Client Permissions: **Default** setting should be **None** with the **Public Folder Visible** checkbox **unchecked**. This setting prevents your top level district public folder from being visible outside of your district.

Note: Do not modify the top level district public folder permissions. To give access to users to administer your public folders, you should modify the membership of the DIST Public Folder Admins security group.

4.4 Advanced Procedures

4.4.1 Edit Extension Attributes

This procedure is used to modify the optional, district-controlled extension attributes of mail-enabled objects.

Note: *You should only edit attributes 1 through 5. Attributes 6 through 15 are reserved for KDE use only*.

a. Open ADUC and navigate to the OU that contains the object.

b. Double-click on the object to open the dialog box.

c. Click on the **Exchange Advanced** tab.

d. Click on the **Custom Attributes** button.

e. Click on the desired attribute and click **Edit**.

f. When your changes are completed, click on **OK** in each window to close the dialog boxes.

4.4.2 Add Access to Resource Mailboxes

This procedure is used to grant additional AD users access to an existing AD user's mailbox; typically this is used to grant one or more personal users the ability to open a resource user's mailbox. The new permission will be available the next time the additional user logs into the domain.

Note: These new permissions may take up to four hours to take effect.

a. Open ADUC and navigate to the OU that contains the object with the mailbox (typically, the resource user).

b. Double-click on the object to open the dialog box.

c. Click on the **Exchange Advanced** tab.

d. Click on the **Mailbox Rights** button.

e. Click on the **Add** button to open the dialog box; use the dialog to select the AD user object which should be able to open the mailbox.

f. Back in the **Permissions** dialog, click the checkboxes next to **Full mailbox access** and **Read permissions**. Click **OK** as needed to close the dialog boxes.

4.4.3 Change the Name of a Personal User

This procedure is used to change the name of a personal user, for instance upon marriage. It will affect the name visible in the GAL and address lists, the SMTP e-mail address, and the user name that appears in ADUC.

a. Open ADUC and navigate to the OU that contains the personal user.

b. Double-click on the object to open the dialog box.

c. Update the **First name**, **Last name,** and **Display name** fields as necessary.

d. Click **OK** to close the dialog box.

e. Right-click on the object and choose **Rename**. In the resulting dialog box, update the name as necessary. (This step updates the **Full Name** value that appears as the user name in ADUC; the value used here does not have to be identical to the value in the **Display Name** field).

The provisioning system will create a new e-mail address matching the updated name upon its next execution. ***Note: in rare cases (for instance, if the user object was copied before the Exchange System Management tools were installed), the provisioning system may fail to create the new e-mail address during its overnight execution. In this situation please contact the KETS Service Desk for assistance****.*

The old e-mail address will remain in the system until manually removed.

Note*: there are additional Active Directory attributes that reflect the user's name; if you need assistance modifying these attributes please contact the KETS Service Desk.*

4.4.4 Change the Name of a Resource User

This procedure is used to change the name of a resource user. It will affect both the name visible in the GAL and address lists and the SMTP e-mail address.

a. Open ADUC and navigate to the OU that contains the object.

b. Double-click on the object to open the dialog box.

c. Update the **First name**, **Last name,** and **Display name** fields as necessary.

d. Click on the **Exchange General** tab.

e. Update the **Alias** field as necessary.

f. Click **OK** to close the dialog box.

g. Right-click on the object and choose **Rename**. In the resulting dialog box, update the name as necessary. (This step updates the **Full Name** value).

The provisioning system will create a new e-mail address matching the updated name upon its next execution. The old e-mail address will remain in the system until manually removed.

4.4.5 Create a Secondary Address for a User, Distribution Group, or Mail-Enabled Security Group

This procedure is used to create secondary SMTP addresses for objects; mail sent to these addresses will go to the object to whom the address is attached. Be sure that the suffix for the address is correct; see section 7.3, “E-mail Addresses” for details of e-mail addresses composition. ***Note:*** *You can only carry out this procedure using an AD user that is in the* ***DIST Staff All Mailbox Access*** *security group (for objects in the* ***Staff*** *or* ***Leadership*** *OUs****)*** *or the* ***DIST Students All Mailbox Access*** *security group (for objects in the* ***Students*** *OU).*

a. Open ADUC and navigate to the OU that contains the object.

b. Double-click on the object to open the dialog box.

c. Click on the **E-mail Addresses** tab.

d. Click on the **New** button.

e. Choose **SMTP Address** and click **OK**.

f. Fill in the **E-mail Address** field with the complete SMTP address. Click **OK** and **OK** to close the dialog boxes.

4.4.6 Mass-create Mailboxes

You can mass-create user objects in Active Directory and the automatic provisioning system will create appropriate mailboxes based on OU membership. OET does not recommend or support any particular method for mass-creating objects in Active Directory, but there are various products and methods available to carry out this task.

4.4.7 Create a Sub-OU

You may create your own sub-OUs in order to organize objects; for instance, you can create sub-OUs of the **Students** OU for each of your schools and place students' user objects in these sub-OUs. Before creating sub-OUs please review the information in the *KETS Active Directory OU Naming Standards*, which can be found on the KDE website at:

http://www.education.ky.gov/KDE/Administrative+Resources/Technology/KETS+Help+Desk/How+Tos+and+Standards+Documents/KETS+Active+Directory.htm

As described in Section 3.2.6, objects placed in sub-OUs will behave just like objects placed in their parent OUs. ***Note****: You can only carry out this procedure using an AD user that is in the* ***DIST Support Admins*** *security group.*

4.4.8 Create a Contact

This procedure is used to create contact objects, which are used when you need an e-mail address to be available in the GAL/address lists but mail content will be stored in another system.

Note*: You can only carry out this procedure using an AD user that is in the* ***DIST Staff All Mailbox Access*** *security group (for objects in the* ***Staff*** *or* ***Leadership*** *OUs****)*** *or the* ***DIST Students All Mailbox Access*** *security group (for objects in the* ***Students*** *OU).*

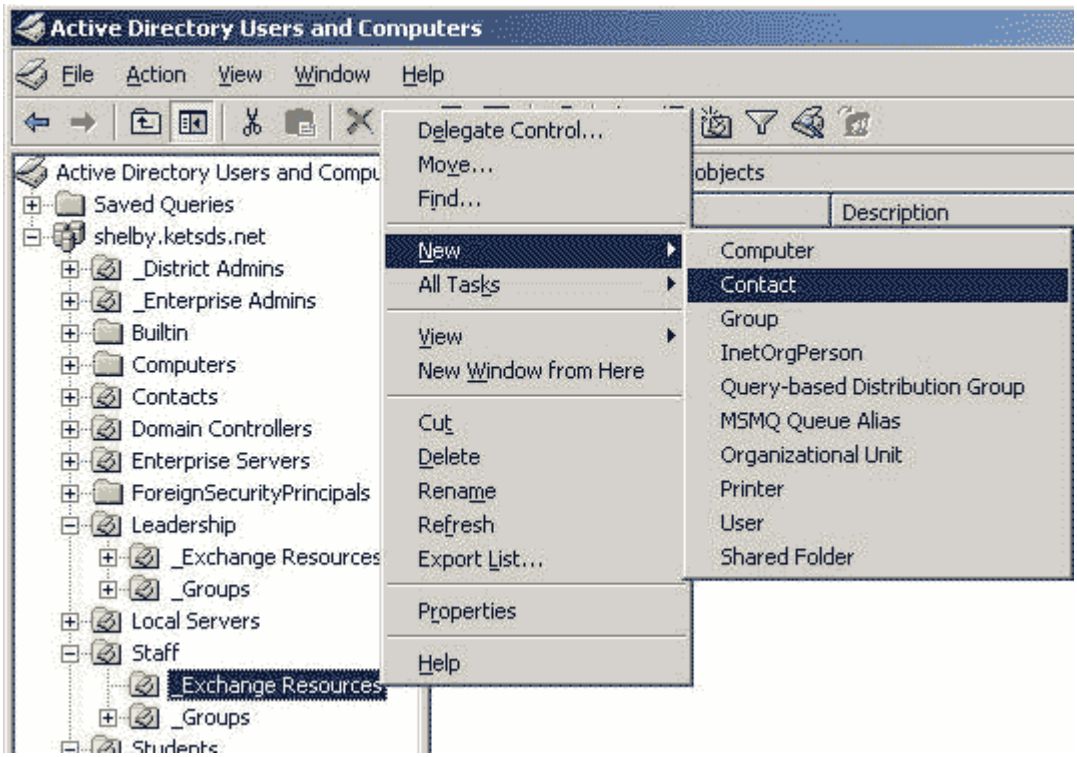
Note: *Contact objects should be created in the (Leadership, Staff, or Students) _Exchange Resources sub-folder for the item to be provisioned correctly. For items to be visible globally, create the contact in Leadership/_Exchange Resources. Items to be viewed by district users only should be placed in Staff/_Exchange Resources. Items that should to be visible to students are to be placed in the Students/_Exchange Resources****.***

a. Determine the OU for the new contact viewable by students (students/_Exchange Resources) based on the OU descriptions above. You may want to use a sub-OU of one of the defined OUs.

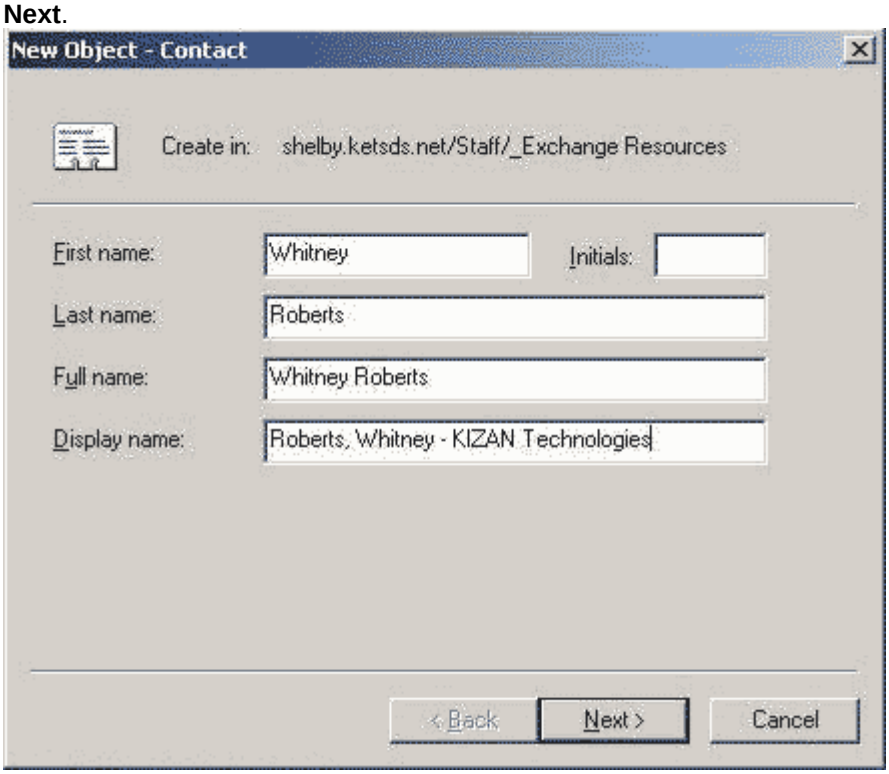
b. Open ADUC and navigate to the chosen OU.

c. Right-click on the chosen OU and choose **New > Contact**.

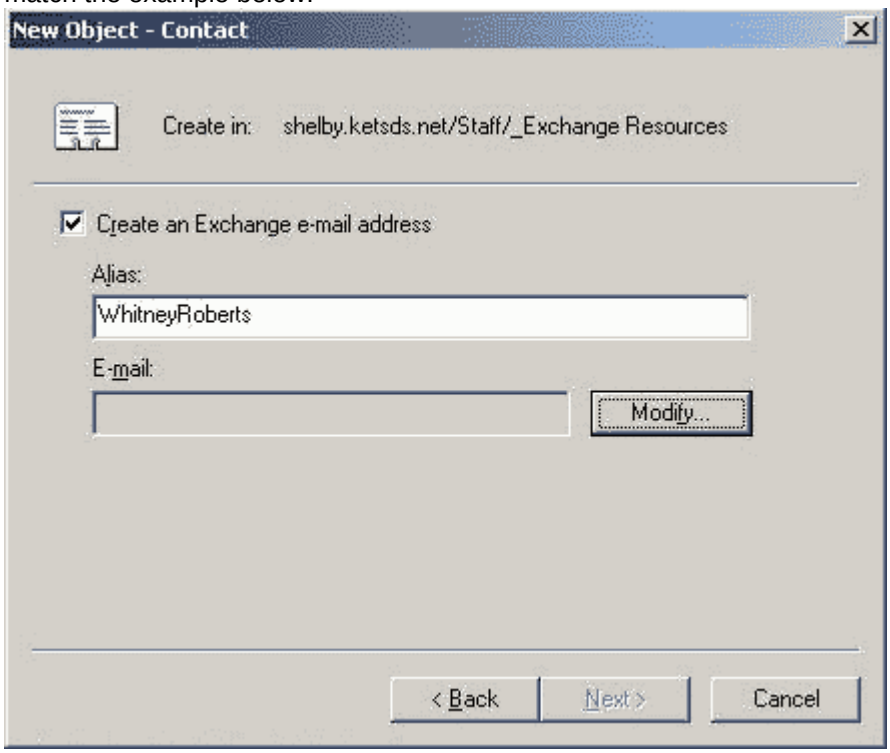
`



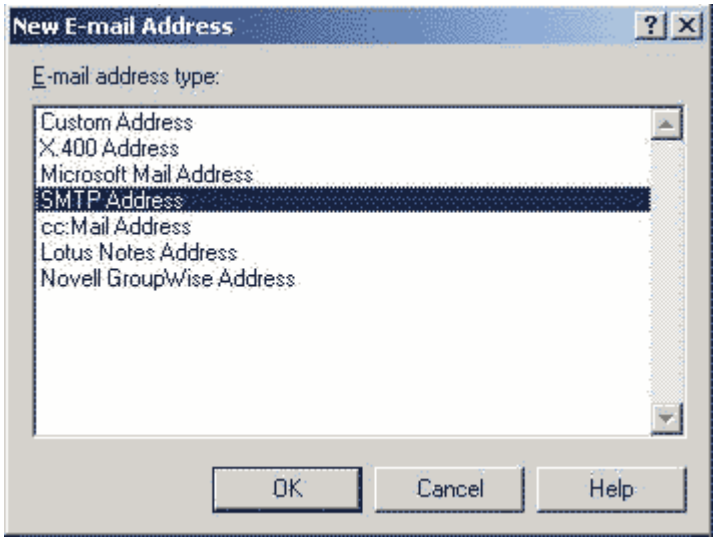
d. Fill in the **First Name** and **Last Name** fields. The **Full Name** field will be filled in automatically. If you don't fill in the **Display name** field, it will be populated with a copy of the **Full name** field after you finish the creation process; if you want the **Display name** to contain additional information to help identify the contact, you may fill it in now. Click **Next**.



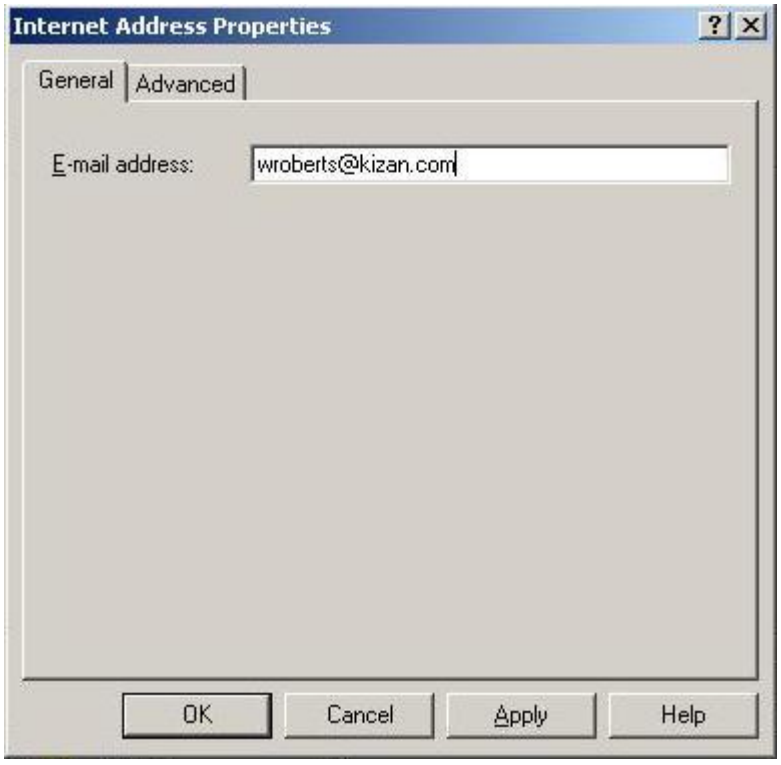
e. Click the **Modify** button. Note: Do not change the checkbox, even if it doesn't match the example below.



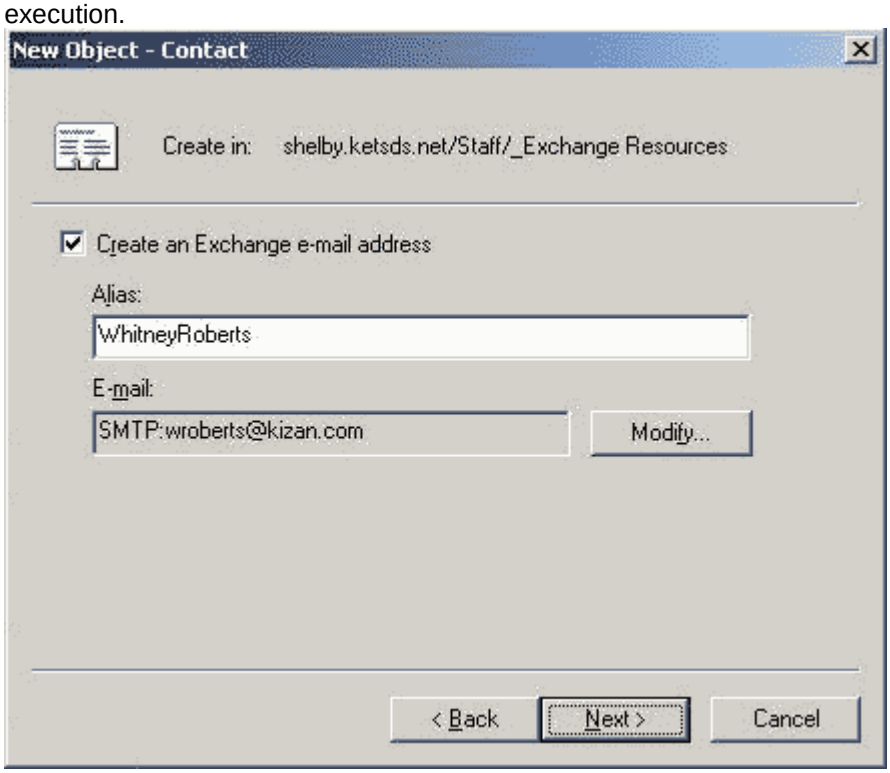
f. Choose **SMTP Address** and click **OK.**



f. Fill in the **E-mail Address** field with the complete SMTP address for the object. Click **OK**.



g. Click **Next** and complete the creation process. The provisioning system will ensure that the contact appears in the correct GALs and address lists upon its next execution.



4.4.9 Grant Send As Permissions

Use this procedure to give a user the ability to send mail as another user; for instance, to give a school secretary the ability to send messages on behalf of the principal.

In order to carry out this procedure, you must have Advanced Features activated in ADUC; this can be set using the **View** menu.

Note: These new permissions may take up to four hours to take effect.

a. Open ADUC and navigate to the OU containing the user on whose behalf mail should be sent.

b. Double-click on the user object to open the dialog box.

c. Click on the **Security** tab.

d. Choose the user or group which should be able to Send As.

e. Choose **Send As**.

f. Click **OK** to close the dialog box. The user given the Send As permission will need to log out and back on to the domain before the new permissions take effect.

4.4.10 Check Mailbox Size

Please reference Exchange System Manager Section 5.1.1

5 Backups for Disaster Recovery and Archiving

OET will maintain a single night's backup on your Exchange 2003 Server for basic disaster recovery purposes which resides on the Exchange Server, but you are responsible for arranging for any additional backups you want additional DR backups or for archival purposes or to protect against a site-wide disaster. You are also responsible for making backups for and carrying out any user data recovery.

5.1 Background

5.1.1 Exchange Backup

Districts will have 1 day of backups stored on the Exchange server in the ExBackups share. The DIST Support Admins group will have permissions to backup the file from this share. The share is named **\\exchangeservername\ExBackups** the name of your exchange server is **ED*nnn*X1** where ***nnn*** is your school district number.

Due to the disaster recovery data being stored on the same server it is **STRONGLY** encouraged for every district to take ownership and routinely copy this file off to another location on the district network or on an external drive. **This will help in the case of a severe hardware failure. If the district has not copied the backup file off to another location, ALL mail will be lost.**

5.1.2 Disaster Recovery Backups

One night's backup exists on each Exchange Server. In the event of a database disaster it is possible to utilize this backup for recovery. BUT, in the event that the server is lost, OS corrupt or drives malfunction this SINGLE backup that exists on the server will not be accessible. It's the district's responsibility to make copies of this backup (**\\exchangeservername\ExBackups)** off the server, and recommended off site. If a district has copies of this backup they can be utilized for recovery in case of a disaster.

Again, Due to infrastructure limitations, the KETS Exchange 2003 environment does not provide for any off-site backups of your Exchange 2003 data, so a disaster that destroys the Exchange 2003 server will result in total loss of e-mail data. At district discretion, you can arrange for offsite disaster recovery backups using the methods described below for archival backups.

5.1.3 Archival Backups

Archival backups can be important for legal purposes as well as recovery from large-scale disasters. It is the district's responsibility to maintain backups, whether for disaster recovery (short-term) or archival (long-term).

If you want additional backups of your Exchange 2003 system for archival purposes, you may make copies of the backup files using the share as discussed above on the Exchange Server. All members of the **DIST Support Admins** security group have read access to the share and its contents.

5.1.4 User Data Recovery

User data recovery means restoring e-mail content for a user or group of users without restoring the entire system to a previous state; for example, restoring a particular message that was accidentally deleted. Exchange 2003 has two features, Deleted Item Retention and Deleted Mailbox Retention, which can be used for user data

recovery in some cases; in other situations recovery is only possible from EXMERGE backups, which are a district responsibility.

5.1.4.1 Deleted Item Retention

Individual mail messages/items that end users delete are actually retained within the Exchange 2003 database and may be recovered up to 14 days after the deletion. This recovery can be performed by end users with the Outlook client software.

5.1.4.2 Deleted Mailbox Retention

Mailboxes that you delete (by adjusting OU membership) are actually retained within the Exchange 2003 database and may be recovered up to 30 days after the deletion. This recovery must be performed by OET.

5.1.4.3 EXMERGE Backups

If you want the ability to use EXMERGE backups to recover user data, you must create and safely store EXMERGE backups. You may want to schedule periodic EXMERGE executions to store all or part of user e-mail content. More information about create and restoring from EXMERGE backups may be found in the video referenced in section 5.1.2, “EXMERGE.” EXMERGE backups are a district responsibility.

5.2 Procedures

5.2.1 Initiate Disaster Recovery

If OET detects that your Exchange 2003 system is not operating correctly and requires disaster recovery, OET staff will contact you to coordinate work. If you believe that your Exchange 2003 system needs disaster recovery, please contact the KETS Help Desk to initiate the process.

5.2.2 Recover a Deleted Mailbox

To arrange for recovery of a deleted mailbox, contact the KETS Help Desk. Mailboxes can only be recovered within 30 days of deletion.

5.2.3 Recover a Deleted Item

To recover a deleted item, use the Outlook 2003 “Recover Deleted Items” feature. For more information, search in Outlook 2003 Help for “Retrieve a deleted item”. Items can only be recovered within 14 days of deletion.

5.2.4 Recover Content Using EXMERGE Backups

To recover content using EXMERGE backups, review the video referenced in section 5.1.2, “EXMERGE.” You must have had EXMERGE backups in place before the item was deleted, and have those backup files available, in order to recover content using EXMERGE.

6 Administrative Tools

6.1 Exchange System Manager

Exchange System Manager, the standard utility Microsoft provides for managing Exchange 2003, can be used at the district level to view mailbox sizes along with local and SMTP queues. To install the Exchange System Manager software, please reference section 6.4.1.

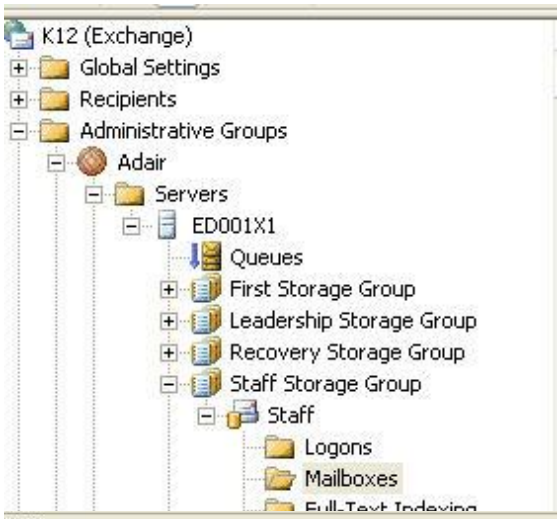
6.1.1 Check Mailbox Size

***Note**: You must be a member of the Dist Exchange Maintenance Reviewers to use System Manager.*

Perform the following to check Mailbox Sizes using the Exchange System Manager:

Open Exchange System Manager by navigating to Start, Programs, Microsoft Exchange, and selecting **System Manager**.

Expand Administrative Groups, Expand the appropriate district, expand Servers, and Exchange server ED ###X1 where ### is the District Number. Select either Leadership or Staff storage group and choose mailboxes. You can sort mailboxes by total size.



Mailboxes

Mailbox	Last Lo...	Size (KB)	Total Items
Redmon, Ruth	ADAIR\...	2,207	88
Reed, Jane	ADAIR\...	14,385	147
Reed, Laura		60,902	894
Reeder, Tammy	ADAIR\...	21,017	276
Reliford, Brett	ADAIR\...	1,082	77
Reliford, Judy	ADAIR\...	19,299	801
Reliford, Pat	ADAIR\...	62,294	632
Reliford, Pete	ADAIR\...	61,150	624
Reliford, Steve	ADAIR\...	31	6
Rexroat, Randy	ADAIR\...	36,385	631
Reynolds, Kevin	ADAIR\...	23,508	80
Rice, Belinda	ADAIR\...	36,809	340
Rich, Alma	ADAIR\...	27,386	395
Rich, Tammy A...	ADAIR\...	18,300	328

You can sort mailboxes by name, size and total items.

6.2 EXMERGE

EXMERGE, the Exchange Mailbox Merge utility provided by Microsoft, has a variety of uses in the KETS Exchange 2003 environment. A version of the utility that works against all versions of Exchange can be downloaded from:

ftp://ketsftp.k12.ky.us/Messaging/E2K3/Exmerge/ExMerge.zip

You should install this utility on the same management workstation on which the Exchange 2003 System Management Tools have been installed. The zip file contents will need to be placed in the C:\Program Files\Exchsrvr\bin folder. If you need assistance downloading or installing the utility, please contact the KETS Help Desk.

You may download a video illustrating various uses of EXMERGE from:

ftp://ketsftp.k12.ky.us/Messaging/Exchange 2003 Project/exmergevideo.zip

This video was made using Exchange 5.5, but the instructions and examples work in the KETS Exchange 2003 environment. One screen (Database Selection) is new in Exchange 2003. On this screen you choose to work with Student, Staff or Leadership mailboxes by choosing the database with the corresponding name. ***Note****: The first database listed (FIRST STORAGE GROUP/MAILBOX STORE) contains system objects, not user mailboxes; do not make any changes in this database.*

Note*: If you need to recover large amounts of data (multiple users mailboxes), please contact the KETS Help Desk prior to running EXMERGE. They will notify OET to turn on circular logging to prevent filling up the log disks. Once you have completed the import using EXMERGE, contact the KETS Help Desk so they can notify OET to turn off circular logging.*

Use this procedure to determine the size of a user's mailbox. *Note: A user can check the size of their own mailbox using features in Outlook.*

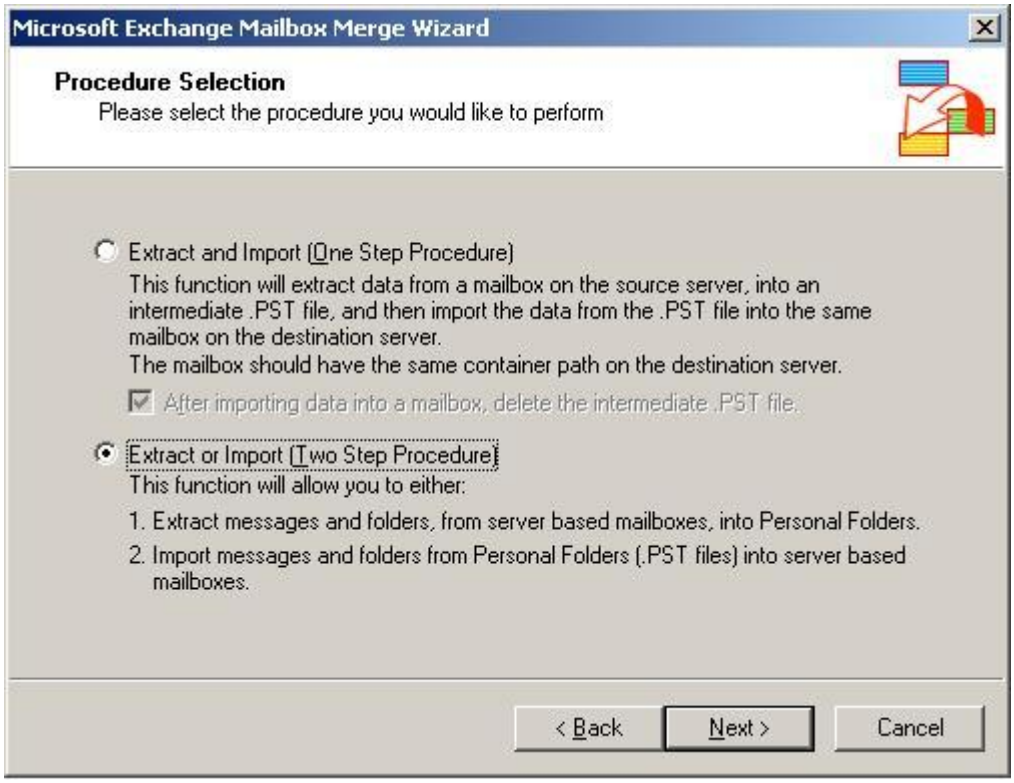
This procedure requires the EXMERGE utility; see section 5.1.2, "EXMERGE", for more information about this utility.

Note*: You can only carry out this procedure using an AD user that is in the* ***DIST Staff All Mailbox Access*** *security group (for objects in the* ***Staff*** *or* ***Leadership*** *OUs****)*** *or the* ***DIST Students All Mailbox Access*** *security group (for objects in the* ***Students*** *OU).*

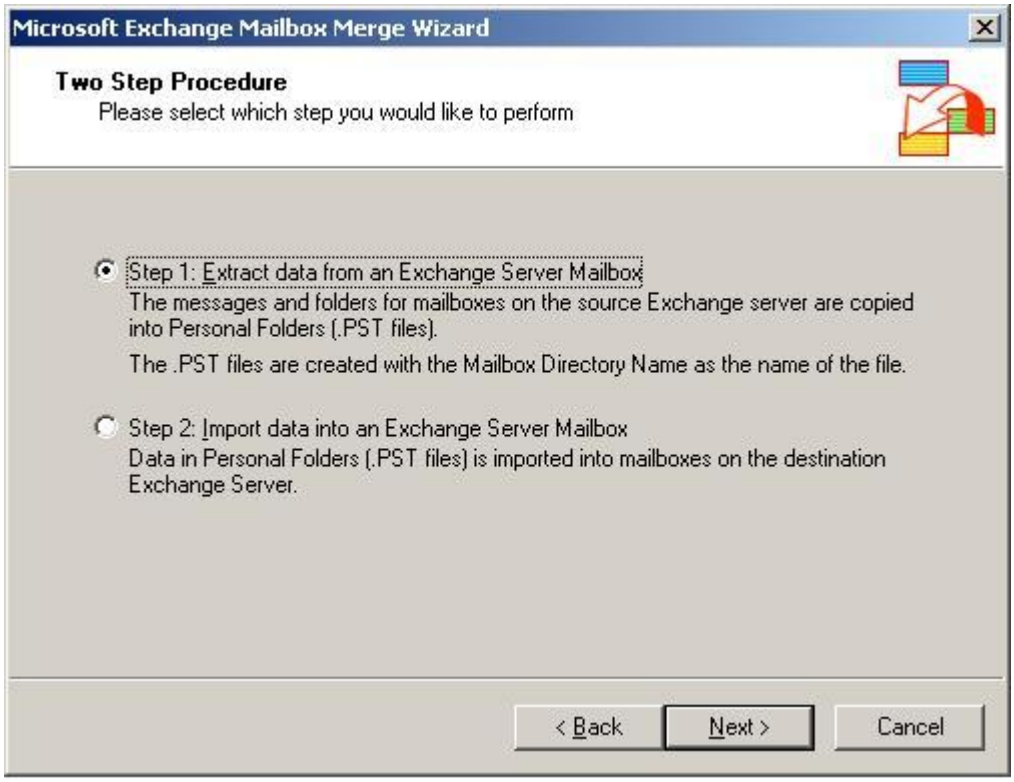
a. Start the EXMERGE utility.

b. Click **Next** on the Welcome screen.

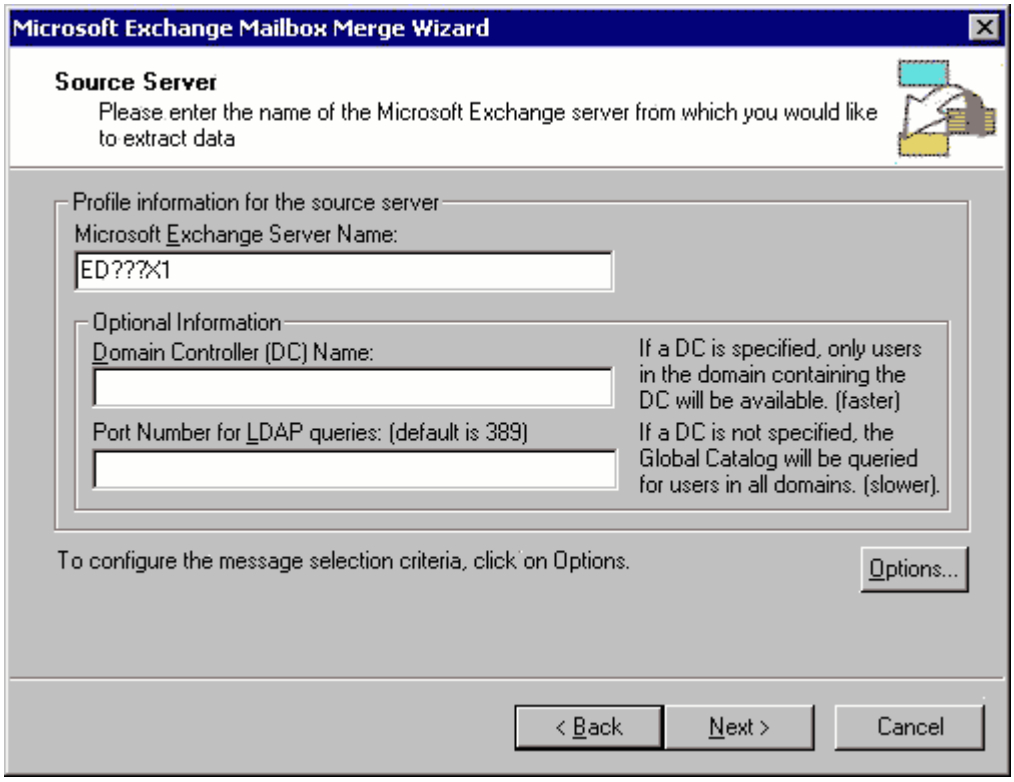
c. On the Procedure Selection screen select the **Extract or Import (Two Step Procedure)** radio button and select **Next**.



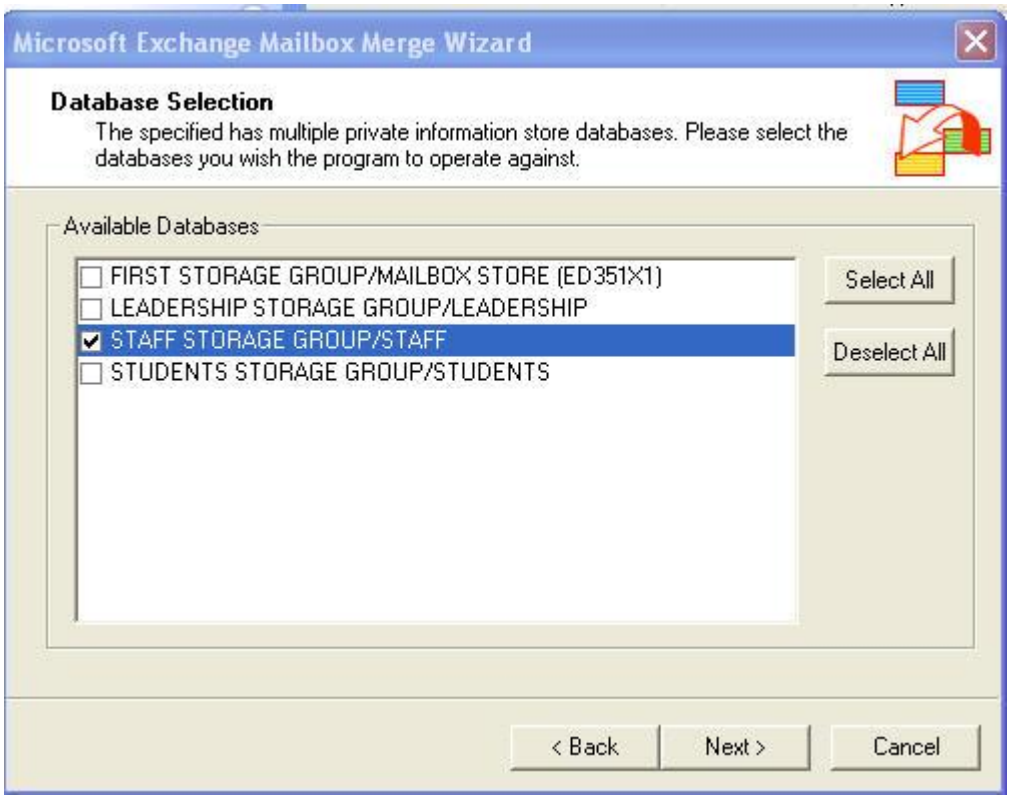
d. On the Two Step procedure screen select the **Step 1: Extract Data from an Exchange Server mailbox** radio button and select **Next.**



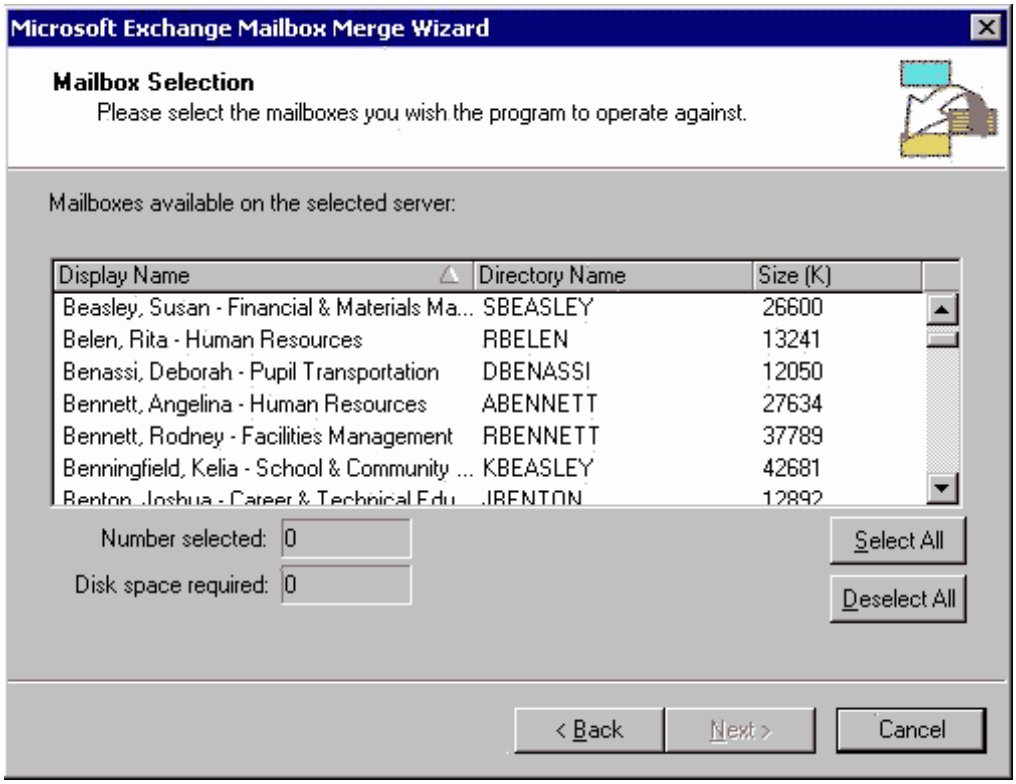
e. Fill in **Microsoft Exchange Server Name** with the name of your Exchange 2003 mailbox server. Do not fill in the other fields. Select **Next**.



f. Choose the appropriate database from the **Available Databases** list and select **Next**. A user's mailbox will be in the database whose name corresponds to the OU of the user. ***Note****: The first database listed (FIRST STORAGE GROUP/MAILBOX STORE) contains system objects, not user mailboxes; do not make any changes in this database.*



g. Note the size of the mailbox of interest. Select **Cancel** to exit out of the EXMERGE utility.



6.3 Active Directory Users and Computers

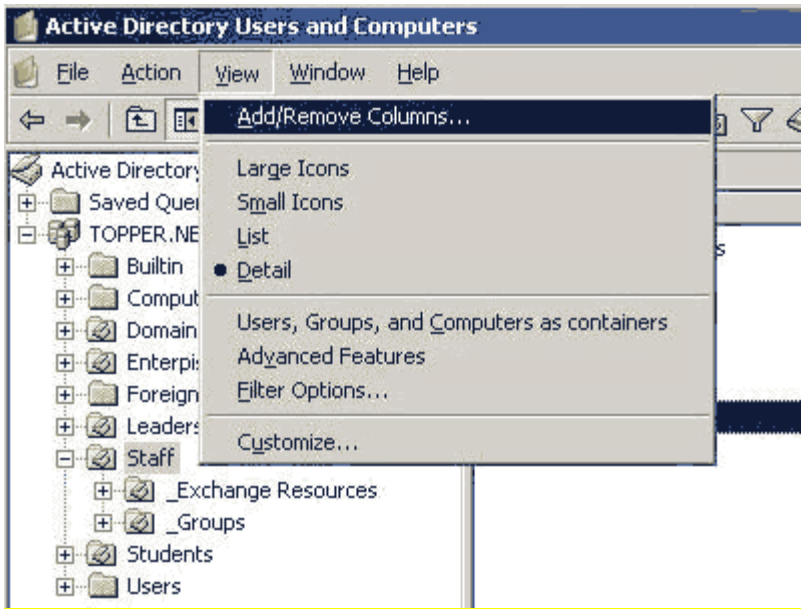
You will carry out most of your Exchange 2003 administrative tasks using the Active Directory Users and Computers utility (ADUC) on a machine with the Exchange 2003 System Management Tools installed (see Section 5.2.1 for step-by-step installation instructions). This section contains brief descriptions of the Exchange-specific screens and dialogs in ADUC. You can reach these screens by finding the desired object in ADUC and double-clicking on it.

6.3.1 Modify Columns Displayed in Active Directory Users & Computers

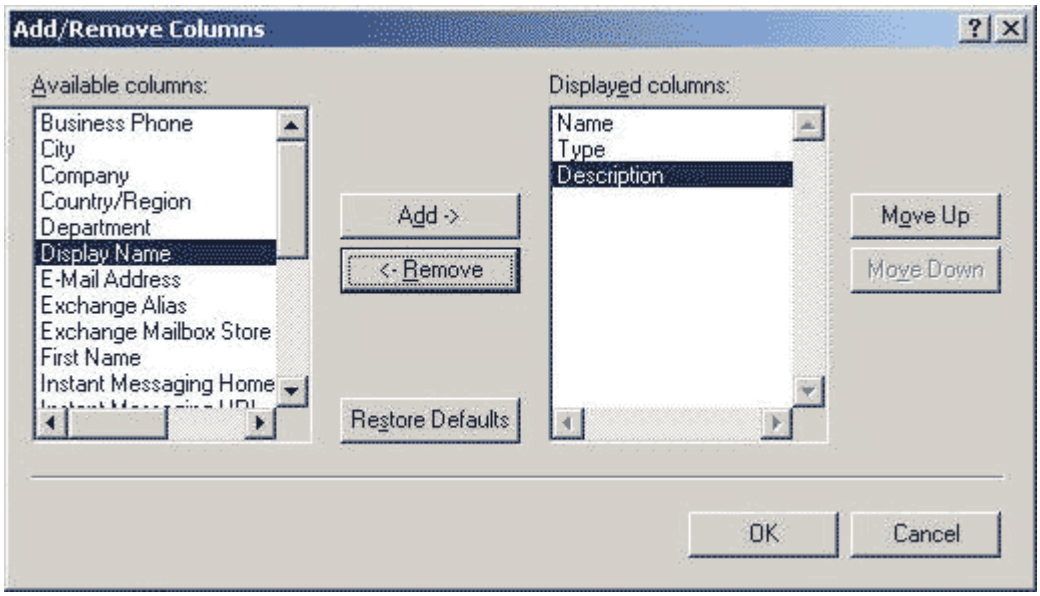
The default set of columns appearing in Active Directory Users & Computers (ADUC) may not include all the information useful in managing Exchange 2003. This procedure is used to modify the default column set.

a. Open ADUC.

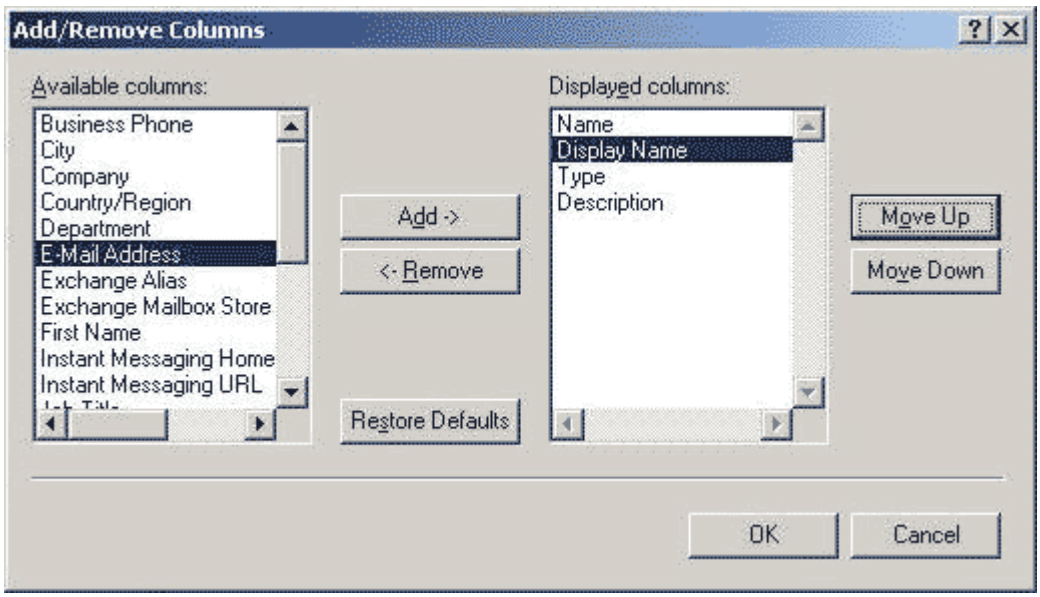
b. Click on **View > Add/Remove Columns…**



c. Choose the columns desired by clicking on entries in the **Available Columns** list and clicking **Add**.

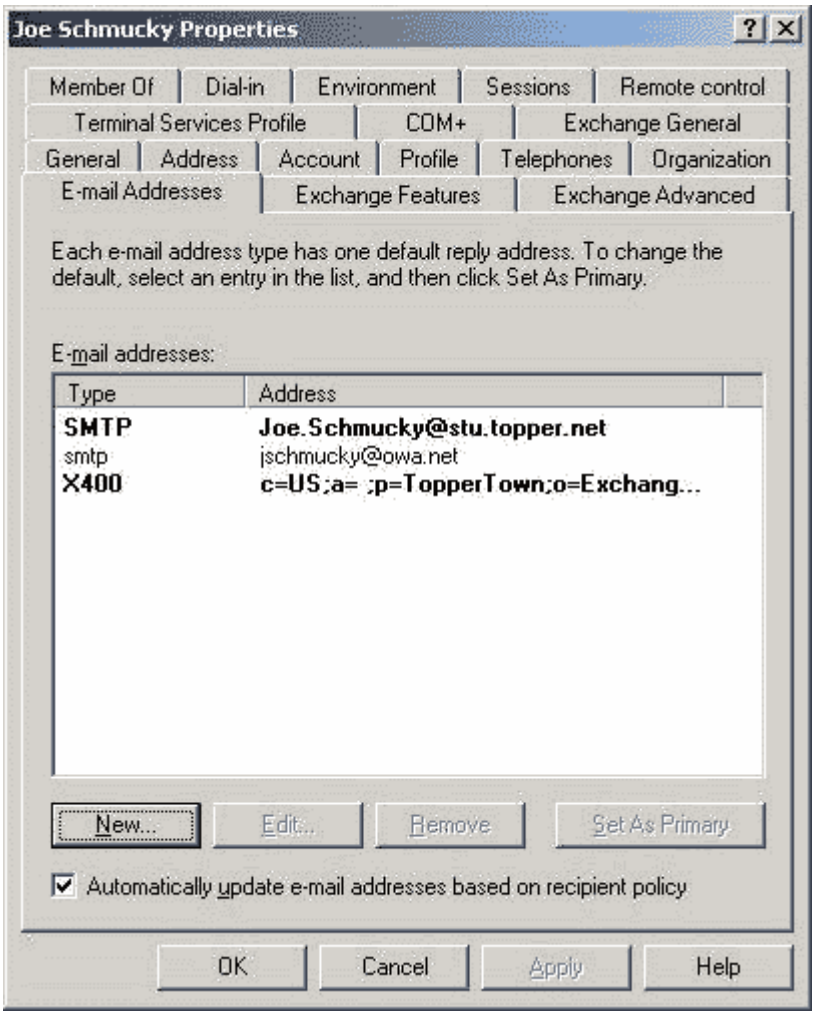


d. When all the desired columns appear in the **Displayed Columns** list, click **OK**.



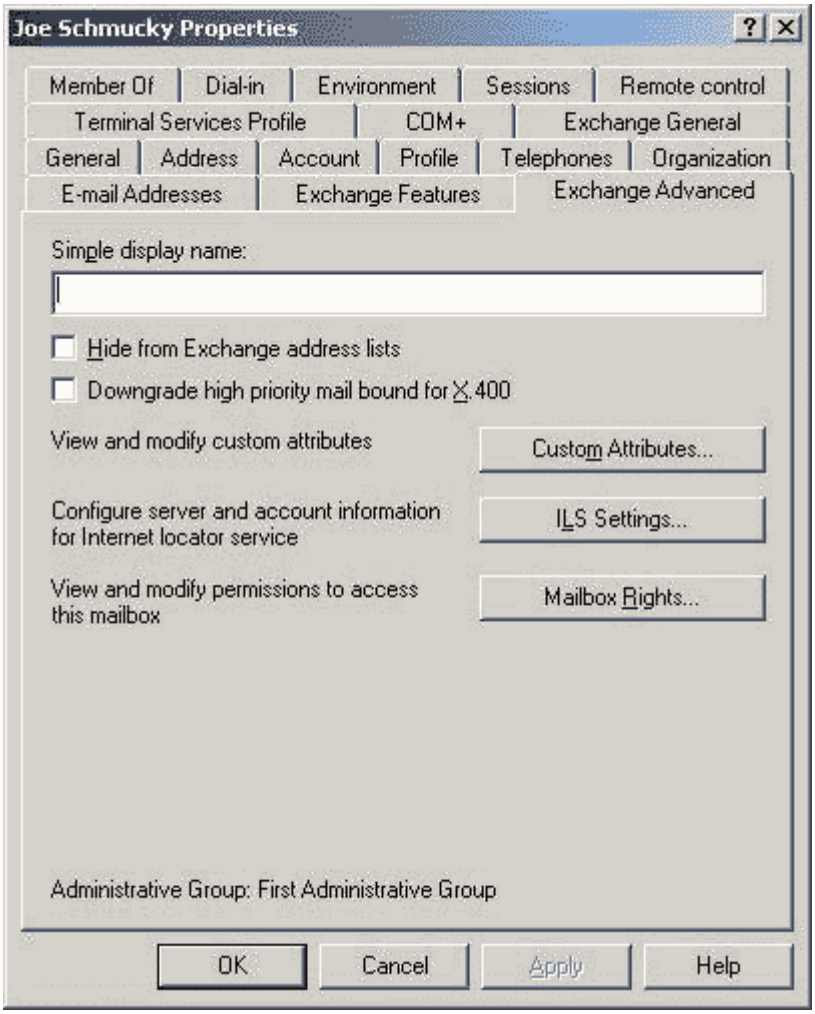
e. The desired columns should now appear.

6.3.2 E-mail Addresses Tab



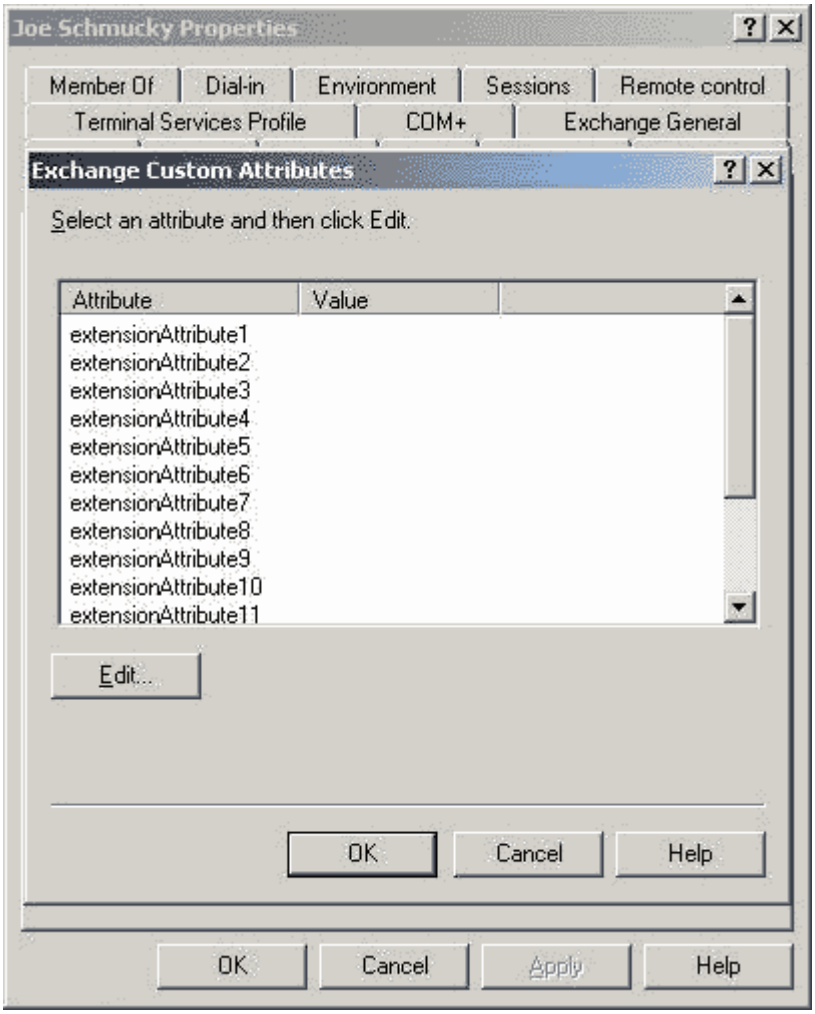
This screen is used to view, edit, add and delete SMTP e-mail addresses for mail-enabled objects. ***Note****: do not change the checkbox at the bottom; depending on the circumstances it may be checked or unchecked, but this is managed by the provisioning script and should not be manually adjusted.*

6.3.3 Exchange Advanced Tab



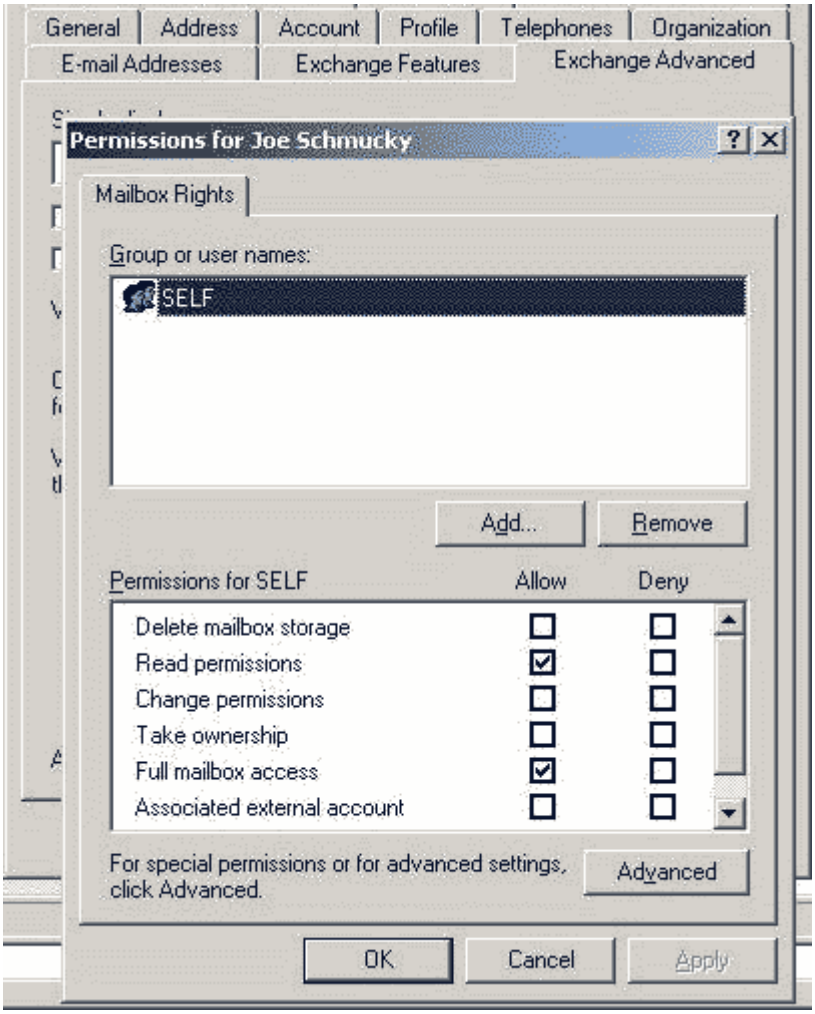
This screen is used to hide objects from all GALs and address lists (but not from IMAP clients like Entourage), and to access other screens.

6.3.4 Exchange Advanced – Custom Attributes



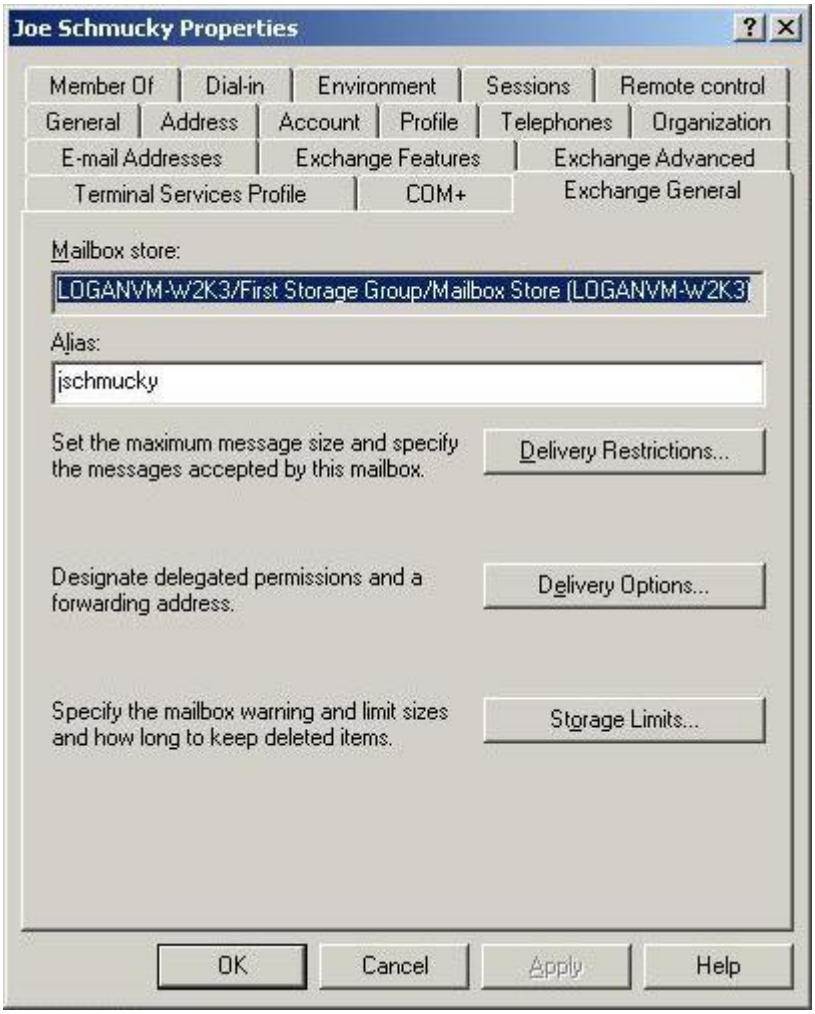
This screen is used to modify custom attributes of mail-enabled objects. *Note: Do not use attributes 6-15 as they are reserved for KDE use.*

6.3.5 Exchange Advanced – Mailbox Rights



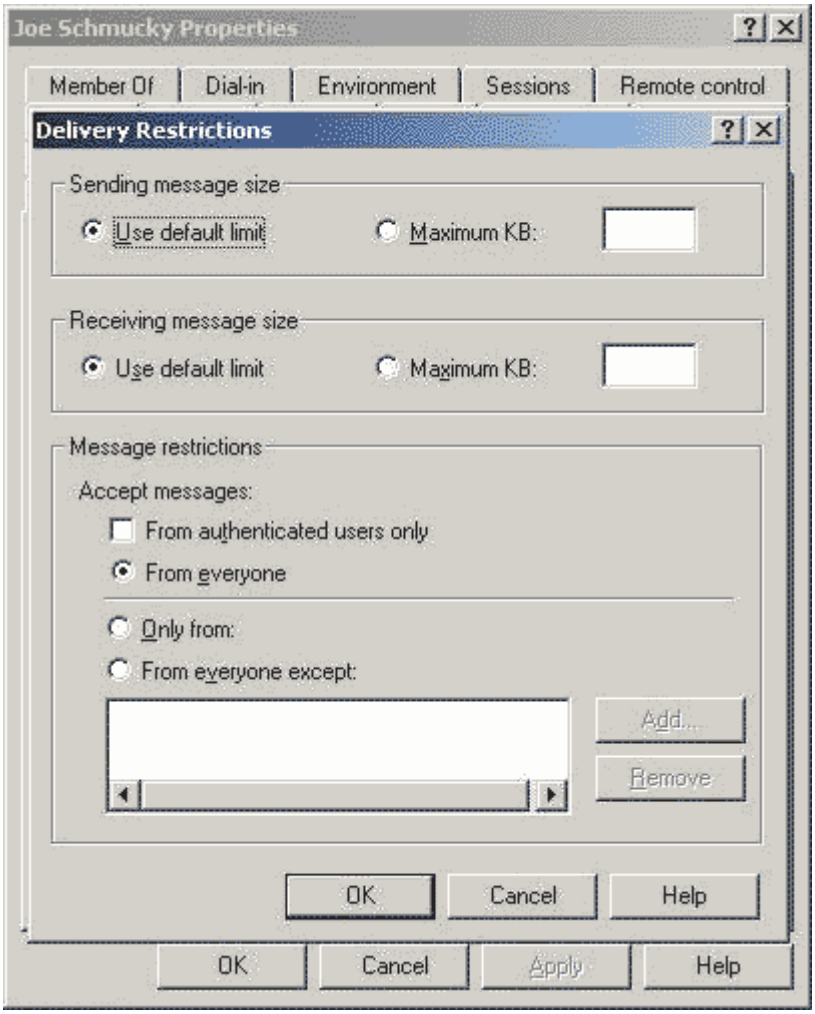
This screen is used to give additional users access to a mailbox, typically for resource users. If you are granting permissions to an additional user, you should grant both **Read permissions** and **Full mailbox access**. ***Note****: Do not change the permissions for* ***SELF****; if you wish to prevent a user from accessing their own mailbox, use the security group membership described in section 3.2.3, "Security Groups."*

6.3.6 Exchange General Tab



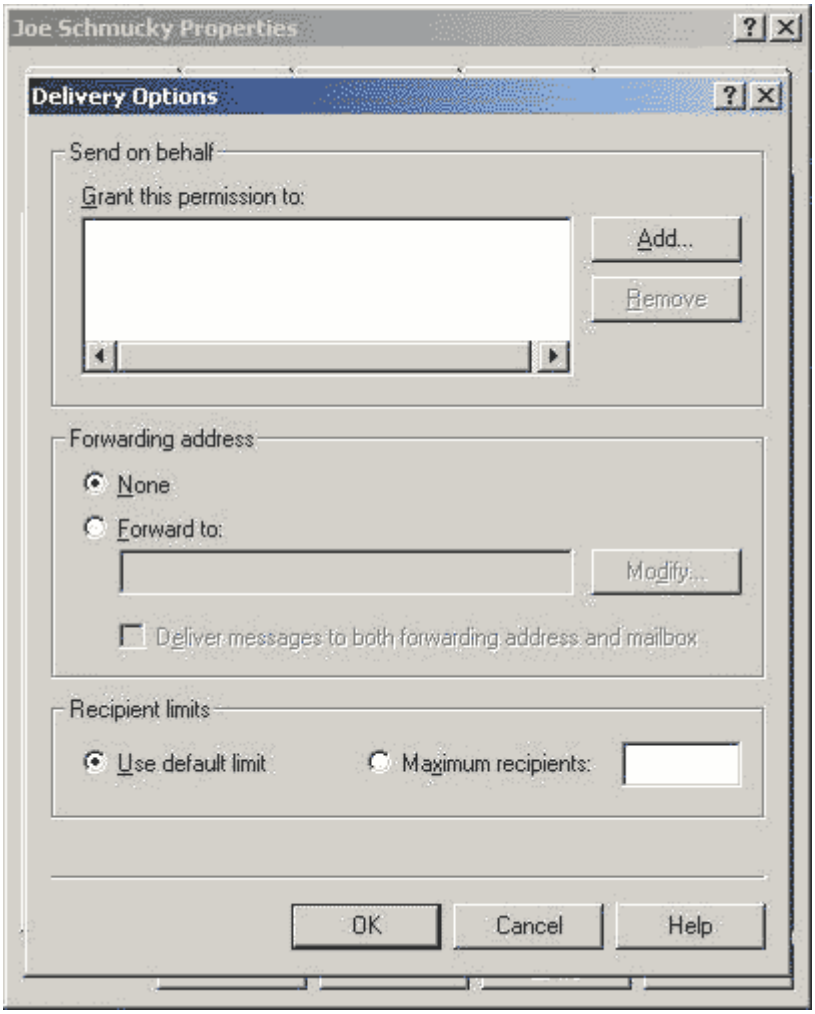
This screen can be used to change the **alias** of a user and access other screens. If both **First name** and **Last name** are blank, the alias is used as the e-mail address prefix.

6.3.7 Exchange General – Delivery Restrictions



This screen is used to override the Enterprise Message Size limit for an individual user. The impacts of such as change are complex, so if you wish to make this change please contact the KETS Help Desk. This screen also allows you to control the users from whom this user can receive e-mail.

6.3.8 Exchange General – Delivery Options



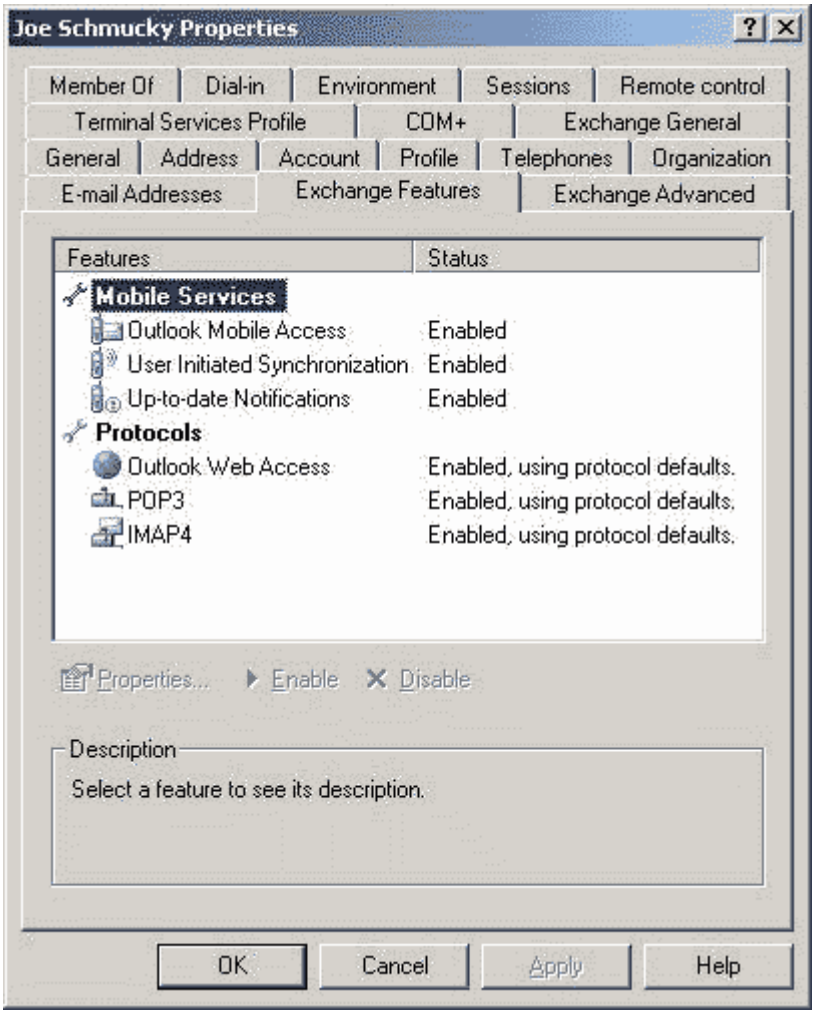
This screen is used to:

Allow a second user to send e-mail on behalf of the chosen user

Create forwarding addresses (which were called Alternate Recipients in Exchange 5.5). ***Note****: unless you click in the checkbox next to* ***Deliver messages to both forwarding address and mailbox,*** ONLY *the forwarding address will receive the message.*

Override the Enterprise Recipient Count limit.

6.3.9 Exchange Features Tab



This screen is used to prevent a user from accessing your Exchange 2003 system over a particular protocol. If you want to completely prevent a user from accessing your Exchange 2003 system, please use the security group as described in section 3.2.3, “Security Groups.”

6.4 Procedures

6.4.1 Install Exchange 2003 System Management Tools

You can install the Exchange 2003 System Management Tools on any Windows XP machine in your domain. The installation files are loaded on the Exchange 2003 server and can be accessed over the network. The logon account you use to install the tools will need administrative access to the machine on which you are installing them.

The Exchange 2003 installer will only work on a machine if the Internet Information Services Snap-In is already installed on the system. IIS does not need to be running to install or use the tools. *If* your machine does *not* have the IIS Snap-in (which would normally be installed along with IIS or can be installed by itself) installed, use the

following steps to install it. ***Note**: You will need access to the Windows XP media in order to complete this procedure.*

a. Click on **Start > Settings > Control Panel.**

b. Double-click on **Add/Remove Programs.**

c. Click on **Add/Remove Windows Components** in the left-hand pane.

d. Select (do not click the checkbox) Internet Information Server and click on **Details**, which opens a new window.

e. Click the checkbox for Internet Information Services Snap-In and click **OK** to close the window.

f. Click **Next** and follow the prompts to install the IIS Snap-In.

Once the IIS Snap-In is installed, use the following steps to install the Exchange 2003 System Management Tools.

g. Click on **Start > Run**.

h. Type *servername*\E2K3Source\SETUP\I386\setup.exe (where *servername* is name of your Exchange 2003 server) and click **OK**.

i. When the Installation Wizard opens, click **Next**.

j. Select 'I agree' and click **Next**.

k. On the Component Selection window, verify that the **Action** for component "Microsoft Exchange" is "Custom" and that the **Action** for component "Microsoft Exchange System Management Tools" is "Install" and click **Next**. If asked to replace a newer file, select No to all.

l. When prompted for the install path, accept the default and click **Next**. The install will begin and will take some time. If an error message pops up about Instant Messenger Admin Service, click **Cancel**. Setup will proceed. Click **Finish** when setup is complete.

The following steps are necessary to install Exchange Service Pack 2.

m. Click on **Start > Run**.

n. Type *servername*\e2k3sp2\setup\i386\update.exe (where *servername* is the name of your Exchange 2003 server) and click **OK**.

o. Accept default choices and click **Next** as necessary to complete the Service Pack installation.

You will now see the Exchange tabs on objects in Active Directory Users and Computers.

7 Client Software & Devices

7.1 Background

7.1.1 Desktop Clients

7.1.1.1 Support

OET aligns its client software support for the KETS Exchange 2003 environment with Microsoft's support. Accordingly, at this time the supported desktop clients are:

- Outlook 2000 SP2 (Windows/Intel)
- Outlook XP (Windows/Intel)
- Outlook 2003 (Windows/Intel)
- Outlook 2001 (Mac)
- Entourage 2004 (Mac)

KETS will support these e-mail clients on the same operating system platforms on which Microsoft supports them.

In addition to these supported clients, the Internet Message Access Protocol (IMAP) may be used to access district Exchange 2003 systems from anywhere inside the KETS network or via KETS Virtual Private Network (VPN), permitting use of other e-mail clients; however, support for these clients is the responsibility of districts.

7.1.1.2 Outlook 2003 Cache Mode

Outlook 2003 has a feature called cache mode, in which the Outlook software keeps a local copy of an end user's mail data. Cache mode can be useful in some situations, but note that global address list/address list functionality is somewhat different and that sent messages actually traverse the network between the client and your Exchange 2003 system twice, once for the message to be sent and again for the message to be placed in the local mail file; this characteristic will increase overall network utilization.

7.1.2 Outlook Web Access

7.1.2.1 Access to Outlook Web Access

The URL for Outlook Web Access (OWA) is:

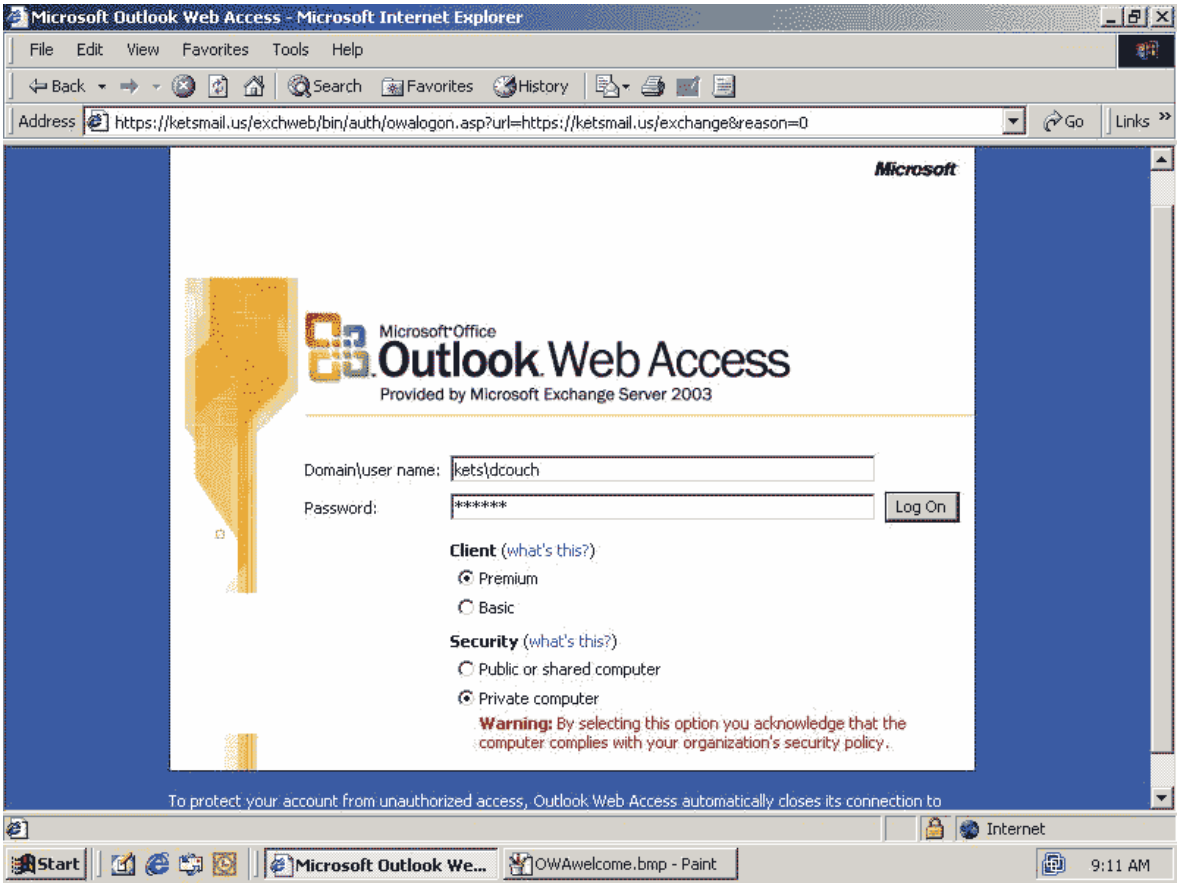
https://ketsmail.us/

This URL is correct for all end users and all network locations (within a district, from home, via VPN, etc.). All communication between the browser and OWA is encrypted using SSL (Secure Sockets Layer). You must ensure that browsers are not using your local http proxy server when accessing OWA. The method for configuring this proxy exception varies by browser; depending on your overall workstation management strategy, you may be able to use Active Directory Group Policies to make this adjustment for Internet Explorer on Windows 2000 and later.

All users will authenticate to OWA using their AD network login credentials, including the domain, in the format *domain\Network logon*; for example, KETS\dcouch.

7.1.2.2 Outlook Web Access Login Screen

The OWA login screen will appear as follows:



The radio buttons allow the end user to choose the type of user interface and the security behavior of the system as follows:

- **Premium** – most sophisticated user interface, with most of the features of the Outlook 2003 desktop client, such as Spell Check, drag and drop, etc. The client computer must have Internet Explorer 5.01 or newer.
- **Basic** – a simpler user interface; this version tends to be more responsive over slow network links and supports a wider variety of browsers. You will not have the enhanced functionality available with the Premium option.
- **Public or shared computer** – this version will automatically end the session after a short amount of inactivity (15 minutes), which is better in shared-computer situations. This is the default setting of the product for security reasons. With this setting, you will be prompted to enter your logon credentials each time the session times out.
- **Private computer** – this version automatically ends the session after inactivity, but with a longer delay (24 hours), and should only be used on non-shared computers. If this is the desired setting, you must select this option each time you logon onto OWA.

NOTE: *Personal folders and the ability to view another person's calendar are not available with OWA.*

7.1.2.3 Support

KETS supports multiple web browsers as OWA clients; some of these browser versions will be able to use all features of OWA. Other browsers may be able to use OWA, in either Premium or Basic version, but are not supported by KETS. Please contact the KETS Service Desk for supported web browsers.

7.1.3 Mobile Devices

7.1.3.1 Support

Mobile device support is enabled in the KETS Exchange 2003 environment so that any device using the Exchange ActiveSync protocol (when configured properly) can access the Exchange 2003 servers. ActiveSync is the inherent Exchange feature for synchronizing handheld devices.

In addition to devices that use ActiveSync, any device that uses a client software redirector to interact with Exchange 2003 may be used. KDE will not configure the KETS Exchange 2003 environment to enable mobile device connectivity to Exchange servers other than via ActiveSync.

Note: *All support of mobile device e-mail functionality is the district's responsibility; KDE will only assist with Exchange 2003 server configuration issues.*

7.1.3.2 ActiveSync Mobile Device Configuration

When configuring ActiveSync devices, set the Servername to KETSMAIL.US, Domain to the user's domain (such as kets), Username to the user's Network logon (such as dcouch), and Password to the user's Active Directory password.

NOTE: *You MUST disable certificate checking on the mobile device*.

If you wish to have traffic between the ActiveSync device and the Exchange 2003 server encrypted in order to protect the user's password and mail content, you must enable SSL in the ActiveSync device; this setting is independent of the certificate checking setting mentioned above.

8 Limits, Standards and Compatibility

8.1 Mailbox Size Limits

Mailbox size limits (measured in megabytes) are based on OU membership of the user as follows:

Mailbox size limit by OU membership

Size limit > OU	Warning	Prohibit Send	Prohibit Send & Receive
Leadership	200	250	300
Staff	45	50	60
Students	5	10	15

There may be legitimate need to increase the mailbox size of some personnel. It is important to note that while this can be done, the management of mailbox size should be the primary responsibility of each individual end user. It is highly recommended as best practice to ensure that there is a limit in place on mailbox size for all users to ensure that mailbox sizes do not grow out of control. Personal Folders can be utilized in Microsoft Outlook to reduce mailbox size and ensure that email messages can be retained. For information relating to personal folder management, see the Appendix A.2.

8.2 Message Size/Recipients Limits

8.2.1 Enterprise Message Size Limit

The enterprise message size limit is 10 MB, which is the Exchange 2003 default. This means that a single message, including any attachments, will only pass through the KETS Exchange 2003 environment (even within a district) if it is 10 MB or less in size. Messages larger than 10 MB will not be sent and the sender will receive a non-delivery report (NDR). Due to the high potential of uncontained growth, which can adversely affect the available amount of storage on local and remote Exchange servers, it is necessary for this limitation to remain in place.

8.2.2 Routing Group Connector Size Limit

Each routing group connector is configured with a 5 MB limit. This means that a single message sized between 5 MB and 10 MB (including any attachments) which is destined outside the originating district will not be sent to its destination during regular business hours. Instead, it will be held by the Exchange 2003 server and sent between 6 PM and 6 AM local time. Messages destined within the district are not affected by this Routing Group Connector limit. If a message is destined to some addresses inside the district and other outside the district, it will be delivered immediately to the in-district addresses and will be queued for out-of-district addresses.

8.2.3 Enterprise Recipient Count Limit

The enterprise recipient count limit is 5000, which is the Exchange 2003 default. This means that a single message originating within the KETS Exchange 2003 environment that is addressed to more than 5000 mail destinations (including each individual member of any distribution groups) will not be sent. An end user attempting to send

such a message will receive an error message. In those cases in which an end user has a legitimate need to send to more than 5000 recipients, you can adjust the limit for that user using ADUC; see section 5.1.3.7, “Exchange General – Delivery Options.”

8.3 E-mail Addresses

8.3.1 Composition

KETS Exchange 2003 environment SMTP e-mail addresses are generated as follows:

District **Leadership**/**Staff** OUs:	*first.last@districtname*.kyschools.us
District **Student** OUs:	*first.last*@stu.*districtname*.kyschools.us
KDE **Leadership/Staff** OUs:	*first.last*@education.ky.gov

If the combination of first name and last name does not create a unique prefix within the district, a number will be appended to the last name (for instance, fred.jones1@somedistrict.kyschools.us). If First Name and Last Name are not populated, the prefix will be the alias (mailnickName); districts may use this approach with resource accounts (such as WEBMASTER).

Legacy e-mail addresses of staff, both KETS standard (*jdoe@district*.k12.ky.us) and non-standard (frank.smith@somedistrict.org), including secondary proxy addresses, will continue to work until August 2007.

Legacy KETS standard addresses for students (*jstudent*@stu.*district*.k12.ky.us) will work until August 2007; legacy non-standard addresses for students (student@somedistrict.org) will *not* function in the KETS Exchange 2003 environment.

NOTE: *In addition to the addresses described above, each user has an SMTP e-mail address ending in **ketsds.net**. These addresses are automatically created by the system to support Outlook Web Access; do not attempt to modify, delete or use these addresses.*

8.3.2 Format

The case of the first name and last name will be preserved in the e-mail address; for instance, if you enter a user’s name as JOE jones, the e-mail address prefix displayed within the system will be JOE.jones. As mentioned earlier, please use mixed case (Joe Jones, not JOE JONES or joe jones) for personal users. However, Exchange 2003 is *not* case-sensitive for e-mail delivery; a message sent to joe.JONES will still be delivered to Joe.Jones.

Most of the characters found on a standard keyboard can be part of an e-mail address. The following characters *cannot* be part of the prefix and if used in the First name or Last name will be stripped out when the e-mail address is generated:

- Any whitespace (space, tab, etc)
- @ - at sign
- (- left parenthesis
-) – right parenthesis
- [- left bracket
-] – right bracket
- \ - backslash

- : - colon
- " – double quote
- ; - semi colon
- , - comma
- < - less-than sign
- > - greater-than sign

8.4 Exchange Server Names

8.4.1 Districts with One Exchange 2003 Server

The naming pattern for districts with a single Exchange 2003 server is

ED*districtnumberOWAFEX*1

where *districtnumber* is the 3-digit district number assigned by KDE.

8.4.2 Districts with Multiple Exchange 2003 Servers

Certain districts with large numbers of e-mail users have multiple Exchange 2003 servers. The naming pattern is

Staff Mailboxes:	ED###X1
Student Mailboxes:	ED###X2
Outlook Web Access:	ED###OWAFEX1

where ### is the 3-digit district number assigned by KDE.

***Note**: The Outlook Web Access machine name is* not *used when trying to access e-mail using a browser.*

8.5 Service Accounts

Most of the server software in the KETS Exchange 2003 environment execute under LocalSystem accounts, though in a few cases other accounts are used. All service accounts will be managed by OET and should not be used or modified by districts; you should place administrators' accounts into appropriate AD security groups to give them any access they need.

8.6 SMTP Relay Support

SMTP Relaying means configuring a mail system to accept messages on port 25 which are destined for another server. This feature is usually used by an application (such as a batch system or monitoring system) which needs to originate e-mail messages but does not have all the mail functionality to determine the proper final destination server for those messages. By default, Exchange 2003 systems in the KETS Exchange 2003 environment will *not* be configured for SMTP Relaying and you cannot change this configuration yourself. If you need this feature configured, please contact the KETS Service Desk.

Please note that ordinary use of Exchange 2003 by client software such as Outlook, Outlook Web Access, etc. does NOT require SMTP Relaying.

9 Address Lists

The ability of end users to see particular e-mail objects (users, distribution groups, mail-enabled security groups, contacts, and public folders) in their client software depends on the OU membership of the object viewed, the OU membership of the end user, and the client software used. Section 3.2.6, "Organization Units", describes the OUs into which e-mail objects can be placed and the effects on visibility; this section will describe the other factors and provide other information about the global address lists (GALs) and address lists.

9.1 Background

9.1.1 Overview of Visibility

The following chart illustrates the visibility situation for most end users. For more details and exceptions, see the following sections.

Visible destinations by type of viewing end user and client software

Viewing End User > / **Client software**	**Staff**	**Students**
MAPI (Outlook 2000, Outlook 2003, etc.) – no cache mode	Statewide staff (including All districts, KDE, and State Agency Staff) Own-district students Own-district staff resource user accounts	Own-district student l users Own-district student resource users
MAPI (Outlook 2003) cache mode – online	Own-district staff Own-district staff resource accounts Own-district students	Own-district student users
MAPI (Outlook 2003) cache mode – offline	Depends on the chosen Offline Address Book	Depends on the chosen Offline Address Book
Outlook Web Access	Own-district staff personal users Own-district staff resource users	Own-district student users
IMAP (Entourage, etc.)	All items in AD	All items in AD

9.1.2 Address List Hierarchy in Outlook

The layout of the address lists as viewed from Outlook clients is hierarchical; each district's **Staff** address list is listed under "All Address Lists", with other address lists for the district indented the **Staff** list. Note that the layout (as well as the membership) is different using other clients.

The example below shows what a Caldwell staff end user will see when using Outlook; this end user can see all address lists for Caldwell, including Caldwell students, but can only see the **Staff** address list for any other district.

Example of Address Lists using Outlook in the KETS Exchange 2003 environment

9.1.3 Outlook Offline Address Books

If you are using Outlook 2003 in offline cache mode, you will have to choose a single address list to be downloaded to your computer. When you open the Address Book in Outlook 2003 in offline mode, Outlook will display the same hierarchy of address lists (including your global address list) that you see in online mode, but if you attempt to chose an address list that was not previously chosen as the Offline Address Book you will receive an error message.

9.1.4 Details of Address Lists/Global Address Lists

This section contains an advanced, detailed explanation of the membership and visibility of the various address lists and global address lists.

9.1.4.1 Hierarchy of Address Lists

The KETS Exchange 2003 environment uses a hierarchy of address lists to organize e-mail destinations by district and by groups within each district. This hierarchy is described below. Note that a given e-mail destination can appear in more than one address list. Address lists only appear in MAPI clients such as Outlook.

- ***District* Staff** – one for each district. This list is at the head of each district hierarchy to support control of address list visibility.

- **Staff & Resources –** one for each district, displayed indented below the ***District* Staff** list
- **Staff & Resources & Students** – one for each district, displayed indented below the ***District* Staff** list.
- **Students** – one for each district, displayed indented below the ***District* Staff** list.

- **KDE**– only one**.**
- **Staff & Resources** – only one; despite the name, this list contains KDE items as described below.

9.1.4.2 Membership in Address Lists

This section explains what e-mail destination objects (users, contacts, groups, public folders) appear in each of the address lists described above. The address lists appear across the top of the table, and the OUs appear in the left-hand column. Each address list only contains objects from its own district. Objects in the _**Groups** OU or any of its sub-OUs do not appear in any address list.

District Address List membership related to OU of e-mail destination object

Address List > OU	***District* Staff**	**Staff & Resources**	**Staff & Resources & Students**	**Students**
Leadership	YES	YES	YES	NO
Leadership - _Exchange Resources	YES	YES	YES	NO
Leadership – Custom subOUs	YES	YES	YES	NO
Staff	YES	YES	YES	NO
Staff - _Exchange Resources	NO	YES	YES	NO
Staff – Custom SubOUs	YES	YES	YES	NO
Students	NO	NO	YES	YES
Students - _Exchange Resources	NO	NO	NO	NO
Students – Custom SubOUs	NO	NO	YES	YES

KDE Address List membership related to OU of e-mail destination object

Address List > OU	KDE	Staff & Resources
Leadership	YES	YES
Leadership - _Exchange Resources	NO	YES
Leadership – Custom subOUs	YES	YES
Staff	YES	YES
Staff - _Exchange Resources	NO	YES
Staff – Custom SubOUs	YES	YES

9.1.4.3 Membership in Global Address Lists

The KETS Exchange 2003 environment uses a series of global address lists so that different end users can focus on the appropriate set of e-mail destinations. The lists are described below; these list names are only visible when choosing a default address list in a MAPI client such as Outlook 2003.

a. District **Staff** – one for each district, contains

- User objects from all **Leadership** OUs statewide (including KDE)
- All KDE-required Distribution Groups (from the **_Exchange Resources** OU within **Leadership)** statewide
- User objects from all sub-OUs of **Leadership** statewide (including KDE) EXCEPT _**Exchange Resources** and _**Groups**
- All objects from the district's **_Exchange Resources** OU within **Leadership**
- User objects from all **Staff** OUs statewide (including KDE)
- User objects from all sub-OUs of **Staff** statewide (including KDE) EXCEPT _**Exchange Resources** and _**Groups**
- All objects from the district's **_Exchange Resources** OU within **Staff**
- User objects from the district's **Students** OU
- User objects from all sub-OUs of the district's **Students** OU EXCEPT _**Exchange Resources** and _**Groups**

b. District **Students** – one for each district, contains

- User objects from the district's **Staff** OU
- User objects from all sub-OUs of the district's **Staff** OU EXCEPT _**Exchange Resources** and _**Groups**
- User objects from the district's **Leadership** OU
- User objects from all sub-OUs of the district's **Leadership** OU EXCEPT _**Exchange Resources** and _**Groups**
- User objects from the district's **Students** OU

- User objects from all sub-OUs of the district's **Students** OU EXCEPT **_Groups**
- All objects from the **_Exchange Resources** OU within the district's **Students** OU

c. KDE – one for KDE, contains

- User objects from all **Leadership** OUs statewide (including KDE)
- All KDE-required Distribution Groups (from the **_Exchange Resources** OU within **Leadership)** statewide
- User objects from all sub-OUs of **Leadership** statewide (including KDE) EXCEPT **_Exchange Resources** and **_Groups**
- User objects from all **Staff** OUs statewide (including KDE)
- User objects from all sub-OUs of **Staff** statewide (including KDE) EXCEPT **_Exchange Resources** and **_Groups**
- All objects from the **_Exchange Resources** OUs within KDE's **Leadership** and **Staff** OUs

9.1.4.4 Address List/Global Address List Visibility

The address lists and global address lists that a given person can see depend on the e-mail client used and the OU membership of the AD user the person used to connect to the email system (the OU membership of the mailbox they are accessing is not significant). The various possibilities are illustrated below. Note that an end user will only be able to see a single GAL but may be able to see multiple address lists.

Login User, Client Software and GAL/AL Visibility

Login User > Client Software	**Member of Staff or Leadership (or sub-OU)**	**Member of Students (or sub-OU)**
MAPI (Outlook 2000, Outlook 2003, etc.) – no cache mode	GAL: ***District* Staff**	GAL: ***District* Students**
	AL: All *district* ALs Every district's **Staff** AL (including KDE)	AL: None (sees hierarchy but no members)
MAPI (Outlook 2003) cache mode – online	GAL: ***District* Staff**	GAL: ***District* Students**
	AL: All *district* ALs Every district's **Staff** AL (including KDE)	AL: None (sees hierarchy but no members)
MAPI (Outlook 2003) cache mode – offline	Any one of the following: ***District* Staff GAL** *District* ALs Other district **Staff** ALs Whichever is chosen to be in the Offline Address Book	***District* Students** GAL
Outlook Web Access	GAL: ***District* Staff**	GAL: ***District* Students**
IMAP (Entourage, etc.)	All items in AD	All items in AD

9.1.5 Public Folder Visibility

The address list/global address list visibility of public folders is not controlled in the same way as the visibility of other objects. By default public folders do not appear in any address list or global address list; if you need a public folder to appear in these lists, please contact the KETS Help Desk.

NOTE: Do not modify the top level district public folder (i.e. "Adair") permissions. The owner for each district top level public folder should be the **Dist Public Folder Admins** security group. You can modify the membership of this group to give users access to administer your public folders.

9.2 Procedures

9.2.1 Hide an Object from Address Lists

Use the following procedure to hide a mail-enabled object from all address lists and GALs. This procedure can be used regardless of the OU membership of the object. *Note: This procedure will* not *hide the object from an IMAP e-mail client such as Entourage.*

a. Open ADUC and navigate to the OU containing the object.

b. Right-click on the object and click **Properties**.

c. Click on the **Exchange Advanced** tab.

d. Click the **Hide from Exchange address lists** checkbox.

e. Click **OK.**

10 SPAM Filtering and Virus Protection

10.1 SPAM Filtering

10.1.1 Background

This section describes SPAM filtering, intended to prevent end users from receiving unsolicited bulk e-mail. OET is providing multiple layers of SPAM filtering systems.

10.1.1.1 Layers

a. Exchange Hosted Services (EHS) – EHS is a service provided to the districts as a means to mitigate the amount of spam or unwanted email from entering the KETS network and reaching the end user. EHS provides the district a means to manage the majority of emails that enter their domain through the use of policy filters, spam quarantines, and routing rules. Each district has been provided a means in which to access the EHS console for their domain. This access allows for both district level support and the ability to customize how their users deal with unwanted email before reaching the end user.

Through EHS, districts will also have the ability to track messages entering or leaving the EHS network to determine where a message has been routed if that message did not reach the intended recipient. This gives the district a means to investigate issues related to email and have an immediate answer to determine if the message was in fact received and set for delivery.

Through the use of spam quarantines, EHS administrators within the district can assist users in acquiring email that may have been misidentified as unwanted email by logging into that user's spam quarantine and ensuring that those messages will no longer be flagged as unwanted. This happens occasionally with newsletters, or subscription services that the user has identified as wanted email.

Policy filters allow a district to edit domains or message types from entering their district. It can also ensure that the specific messages be sent through pending that they setup a white list or an allowed email sender list as a policy.

Districts will also have the ability to run reports against their particular domain for management purposes to show the amount of threats blocked by EHS and the number of unwanted messages being filtered by policies setup both at the district level and KDE level.

b. Outlook Intelligent Message Filtering – Outlook 2003 (in cache mode) has built-in capabilities to delete or file messages based on their composition. Configuration is at the discretion of each district.

10.2 Virus Protection

10.2.1 Background

10.2.1.1 Layers

OET provides the following layers of virus protection.

a. Enterprise GroupShield - OET uses McAfee GroupShield to block messages containing viruses, or attachments with dangerous file types, at the entry point to the KETS Exchange 2003 environment.

b. District GroupShield - OET uses McAfee Groupshield to block messages containing viruses, or attachments with dangerous file types, on each district's Exchange 2003 system.

c. OET uses McAfee VirusScan to protect the operating system and software installed on Exchange systems from viruses.

Appendix A – Mailbox Management – Best Practices

A.1 Increasing Student and Staff Mailbox Capacity

In certain circumstances, it may be necessary to increase the mailbox size of a staff or group of staff or students. While this is at the district's discretion, it is important to note that the there should be a practical limitation set for the mailbox size. Some consequences of not placing restrictions on mailboxes can cause database file sizes to increase, along with backups and backup copies to take longer and increase dramatically in size.

Student accounts should be left in the Student OU. Placing a student in the Staff OU would result in the student's email address to be visible in the Global Address List.

For staff or students that require a larger mailbox capacity, it is recommended that the adjustment of the mailbox size be edited on the AD object.

A.2 Personal Folders

With the use of Outlook Desktop clients, such as Outlook 2003, mailbox content can be stored in Personal Folders. The use of personal folders is paramount to the reduction of mailbox size and providing a repository for messages that the user can maintain.

Sub-folders can be created below the personal folder, which will assist the user in organizing items. Messages can then be moved to those folders.

Personal folder files can also be stored on the local workstation or a network location such as a staff users share on a remote server.

The education of users and emphasizing the importance of viewing the inbox as a temporary receiving point for messages will aid in the overall reduction of information stores. This will also assist the user in being able to efficiently organize and locate sent and received messages.

A.3 Leadership OU Population

The total number of user objects allowed in this OU is either 10 or 2 times the district workstation allocation (DWA), whichever is higher.

Appendix B

B.1 State Level Distribution Group Checklist

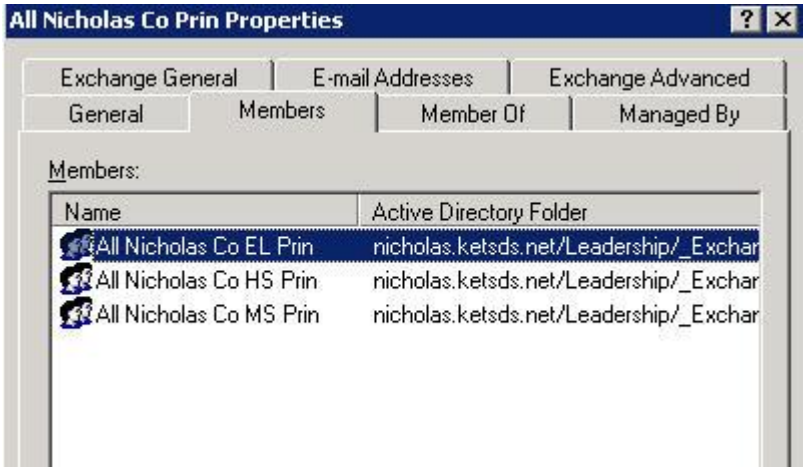
The following statewide distribution groups (DGs) should be located within the Leadership\Exchange Resources OU in Active Directory.

- All *District Name* EL Prin
- All *District Name* MS Prin
- All *District Name* HS Prin
- All *District Name* Prin
- All *District Name* Supt
- All *District Name* EL Teachers
- All *District Name* MS Teachers
- All *District Name* HS Teachers
- All *District Name* IT Teachers
- All *District Name* Teachers

Examples: “All Pike Co EL Prin” or “All Burgin Ind EL Prin”

NOTE: The words, County and Independent, MUST be represented as “Co” and “Ind” respectively with no period. All *District Name* IT Teachers is for District Itinerant Teachers.

All *District Name* Prin



To assign access rights to each distribution list, go to the Exchange General tab of each distribution group and follow steps outlined below:

For All *District Name* Supt

1. Click on the Exchange General Tab.
2. In the "Accept Messages From" window, select "Only from".
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Supt*
   b. *Admin SDL*
5. Click OK and OK again.

For All *District Name* Prin

1. Click on the Exchange General Tab.
2. In the "Accept Messages From" window, select "Only from".
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Prin*
   b. *Admin PDL*
5. Click OK and OK again.

For All *District Name* EL Prin

1. Click on the Exchange General Tab.
2. In the "Accept Messages From" window, select "Only from".
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Prin*
   b. *Admin EPDL*
5. Click OK and OK again.

For All *District Name* MS Prin

1. Click on the Exchange General Tab.
2. In the "Accept Messages From" window, select "Only from".
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Prin*
   b. *Admin MPDL*
5. Click OK and OK again.

For All *District Name* HS Prin

1. Click on the Exchange General Tab.
2. In the "Accept Messages From" window, select "Only from".
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Prin*
   b. *Admin EPDL*
5. Click OK and OK again.

For All *District Name* Teachers

1. Click on the Exchange General Tab.
2. In the “Accept Messages From” window, select “Only from”.
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Teachers*
   b. *Admin TDL*
   (Option: Assign access for other users)
5. Click OK and OK again.

For All *District Name* EL Teachers

1. Click on the Exchange General Tab
2. In the “Accept Messages From” window, select “Only from”.
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Teachers*
   b. *Admin ETDL*
   (Option: Assign access for other users)
5. Click OK and OK again.

For All *District Name* MS Teachers

1. Click on the Exchange General Tab
2. In the “Accept Messages From” window, select “Only from”.
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Teachers*
   b. *Admin MTDL*
   (Option: Assign access for other users)
5. Click OK and OK again.

For All *District Name* HS Teachers

1. Click on the Exchange General Tab
2. In the “Accept Messages From” window, select “Only from”.
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Teachers*
   b. *Admin HTDL*

   (Option: Assign access for other users)
5. Click OK and OK again.

For All *District Name* IT Teachers (for District Itinerant teachers)

1. Click on the Exchange General Tab
2. In the “Accept Messages From” window, select “Only from”.
3. Click the Modify button.
4. Select the following distribution groups:
   a. *All State Teachers*
   b. *Admin ITDL*

   (Option: Assign access for other users)
5. Click OK and OK again.